EXAMTOPICS

-Expert Verified, Online, **Free**.



CERTIFICATION TEST

-CertificationTest.net - Cheap & Quality Resources With Best Support

Question #1 *Topic 1*

Which analysis detonates previously unknown submissions in a custom-built, evasion-resistant virtual environment to determine real-world effects and behavior?

A. Dynamic

B. Pre-exploit protection

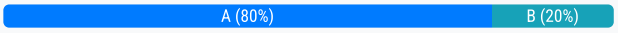
C. Bare-metal

D. Static

Suggested Answer: *A*

Official Answer: A

Community vote distribution



blahblah1234567890000 Most Recent 3 years, 11 months ago

Its A. This also applies to sandbox and wildfire: The WildFire cloud-based malware analysis environment is a cyber threat prevention service that identifies unknown malware, zero-day exploits, and advanced persistent threats (APTs) through static and dynamic analysis in a scalable, virtual environment.

upvoted 1 times

dax 4 years, 5 months ago

Answer is a

upvoted 3 times

error_909 4 years, 5 months ago

WildFire inspection and analysis In addition to local analysis, Cortex XDR can send unknown files to WildFire for discovery and deeper analysis to rapidly detect potentially unknown malware. WildFire brings together the benefits of independent detection techniques for high-fidelity and evasion-resistant discovery that goes beyond legacy approaches. Among these techniques: ● Static analysis is a powerful form of analysis, based in the cloud, that detects known threats by analyzing the characteristics of samples before execution. ● Dynamic analysis (sandboxing) detonates previously unknown submissions in a custombuilt, evasion-resistant virtual environment to determine real-world effects and behavior. ● Bare-metal analysis uses a hardware-based analysis environment specifically designed for advanced threats that exhibit highly evasive characteristics and can detect virtual analysisSorry its AConsistently incorrect.

upvoted 1 times

error_909 4 years, 5 months ago

Selected Answer: B

WildFire inspection and analysis In addition to local analysis, Cortex XDR can send unknown files to WildFire for discovery and deeper analysis to rapidly detect potentially unknown malware. WildFire brings together the benefits of independent detection techniques for high-fidelity and evasion-resistant discovery that goes beyond legacy approaches. Among these techniques: ● Static analysis is a powerful form of analysis, based in the cloud, that detects known threats by analyzing the characteristics of samples before execution. ● Dynamic analysis (sandboxing) detonates previously unknown submissions in a custombuilt, evasion-resistant virtual environment to determine real-world effects and behavior. ● Bare-metal analysis uses a hardware-based analysis environment specifically designed for advanced threats that exhibit highly evasive characteristics and can detect virtual analysis

upvoted 1 times

error_909 4 years, 5 months ago

Sorry its A

upvoted 1 times

blahblah1234567890000 3 years, 11 months ago

Consistently incorrect.

upvoted 1 times

Question #2 *Topic 1*

What is required for a SIEM to operate correctly to ensure a translated flow from the system of interest to the SIEM data lake?

A. connectors and interfaces

B. infrastructure and containers

C. containers and developers

D. data center and UPS

Suggested Answer: *A*
Official Answer: A

Karthik_Krishnamoorthy Most Recent 3 years, 8 months ago

SIEM Connector are used to read various logs and forwarding them to your SIEM Platform in a standardized format. Interfaces are various tool in the SIEM Platform.

upvoted 1 times

Question #3 *Topic 1*

Which type of Wi-Fi attack depends on the victim initiating the connection?

A. Evil twin

B. Jasager

C. Parager

D. Mirai

Suggested Answer: *A*
Official Answer: A

Community vote distribution
A (90%) B (10%)

jshow Highly Voted 5 years, 3 months ago
This should be A: Evil Twin
upvoted 6 times

Amaury93 Most Recent 3 years, 8 months ago
it should be evil twin
upvoted 1 times

blahblah1234567890000 4 years, 1 month ago
Page 62 Study GuideEvil Twin Perhaps the easiest way for an attacker to find a victim to exploit is to set up a wireless access point that serves as a bridge to a real network. An attacker can inevitably bait a few victims with “free Wi-Fi access.” The main problem with this approach is that it requires a potential victim to stumble on the access point and connect. The attacker can’t easily target a specific victim, because the attack depends on the victim initiating the connection.
upvoted 2 times

blahblah1234567890000 4 years, 1 month ago
Selected Answer: A
Page 62 Study Guide
upvoted 2 times

blahblah1234567890000 3 years, 11 months ago
Evil Twin Perhaps the easiest way for an attacker to find a victim to exploit is to set up a wireless access point that serves as a bridge to a real network. An attacker can inevitably bait a few victims with “free Wi-Fi access.” The main problem with this approach is that it requires a potential victim to stumble on the access point and connect. The attacker can’t easily target a specific victim, because the attack depends on the victim initiating the connection.
upvoted 1 times

Merlin0o 4 years, 2 months ago
should be A: Evil Twin https://www.paloaltonetworks.com/blog/2013/11/wireless-man-middle/ "Still, the user has to select the network" With The Jasager attack "The user doesn't have to manually choose the attacker’s access point,"
upvoted 2 times

error_909 4 years, 5 months ago
B is correctwrong its a
upvoted 1 times

error_909 4 years, 5 months ago
Selected Answer: B
B is correct
upvoted 1 times

blahblah1234567890000 3 years, 11 months ago
wrong its a
upvoted 2 times

Bubu3k 4 years, 6 months ago

Should be A, as per study guide, page 62: "The main problem with this approach is that it requires a potential victim to stumble on the access point and connect. The attacker can't easily target a specific victim, because the attack depends on the victim initiating the connection."

upvoted 4 times

Question #4 *Topic 1*

Which term describes data packets that move in and out of the virtualized environment from the host network or a corresponding traditional data center?

A. North-South traffic

B. Intrazone traffic

C. East-West traffic

D. Interzone traffic

Suggested Answer: *A*

Official Answer: A

Community vote distribution

A (100%)

blahblah1234567890000 Most Recent 4 years, 1 month ago

Page 208 study guide

upvoted 1 times

Question #5 *Topic 1*

Which organizational function is responsible for security automation and eventual vetting of the solution to help ensure consistency through machine-driven responses to security issues?

A. NetOps

B. SecOps

C. SecDevOps

D. DevOps

Suggested Answer: *B*

Official Answer: B

Community vote distribution

B (100%)

blahblah1234567890000 4 years, 1 month ago

Selected Answer: B

Page 233 study guide

upvoted 2 times

blahblah1234567890000 4 years, 1 month ago

Page 233 study guideSecurity operations (SecOps) is a necessary function for protecting the digital way of life, for global businesses and customers. SecOps requires continuous improvement in operations to handle fast-evolving threats. SecOps needs to arm security operations professionals with highfidelity intelligence, contextual data, and automated prevention workflows to quickly identify and respond to these threats. SecOps must leverage automation to reduce strain on analysts and execute the Security Operation Center's (SOC) mission to identify, investigate, and mitigate threats.

upvoted 2 times

blahblah1234567890000 **Most Recent** 3 years, 12 months ago

Security operations (SecOps) is a necessary function for protecting the digital way of life, for global businesses and customers. SecOps requires continuous improvement in operations to handle fast-evolving threats. SecOps needs to arm security operations professionals with highfidelity intelligence, contextual data, and automated prevention workflows to quickly identify and respond to these threats. SecOps must leverage automation to reduce strain on analysts and execute the Security Operation Center's (SOC) mission to identify, investigate, and mitigate threats.

upvoted 2 times

DRAG DROP -

Given the graphic, match each stage of the cyber-attack lifecycle to its description.

Select and Place:



reconnaissance		attacker will plan the cyber-attack
weaponization		attacker will determine which method to use to compromise an endpoint
delivery		attacker will distribute their weaponized payload to an endpoint
exploitation		attacker will trigger a weaponized payload
installation		escalate privileges on a compromised endpoint
command and control		establish secure communication channel to servers across the internet to reshape attack objectives

Suggested Answer:

reconnaissance	reconnaissance	attacker will plan the cyber-attack
weaponization	weaponization	attacker will determine which method to use to compromise an endpoint
delivery	delivery	attacker will distribute their weaponized payload to an endpoint
exploitation	exploitation	attacker will trigger a weaponized payload
installation	installation	escalate privileges on a compromised endpoint
command and control	command and control	establish secure communication channel to servers across the internet to reshape attack objectives

reconnaissance	reconnaissance	attacker will plan the cyber-attack
weaponization	weaponization	attacker will determine which method to use to compromise an endpoint
delivery	delivery	attacker will distribute their weaponized payload to an endpoint
exploitation	exploitation	attacker will trigger a weaponized payload
installation	installation	escalate privileges on a compromised endpoint
command and control	command and control	establish secure communication channel to servers across the internet to reshape attack objectives

blahblah1234567890000 Most Recent 1 year, 11 months ago

Answer is correct. Pg 30/31 of the study guide.

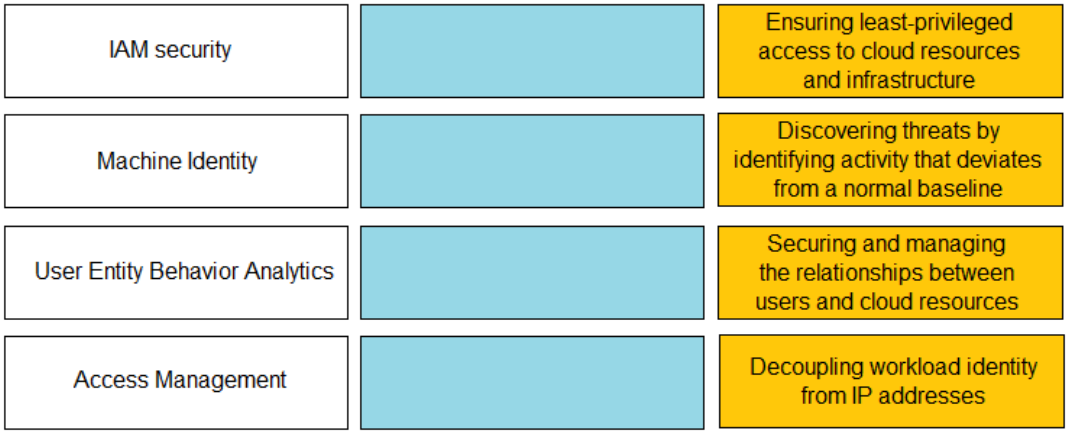
upvoted 2 times

Question #7 *Topic 1*

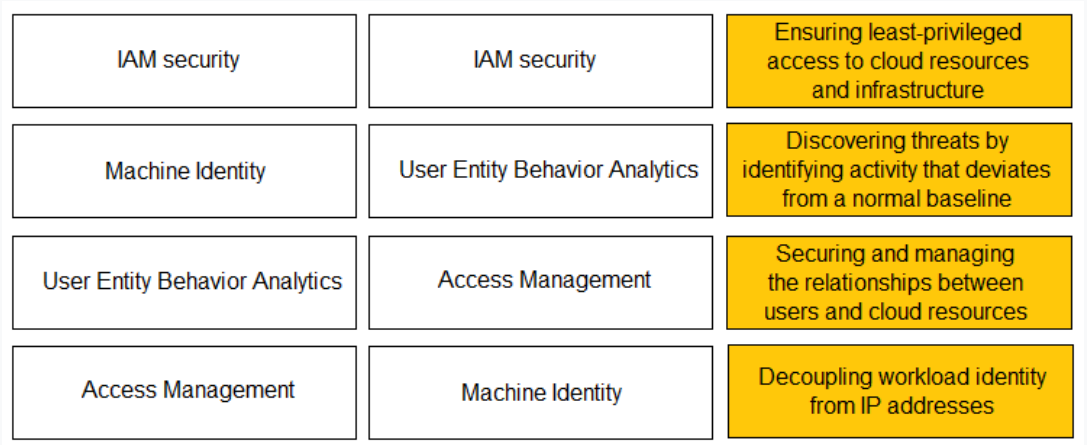
DRAG DROP -

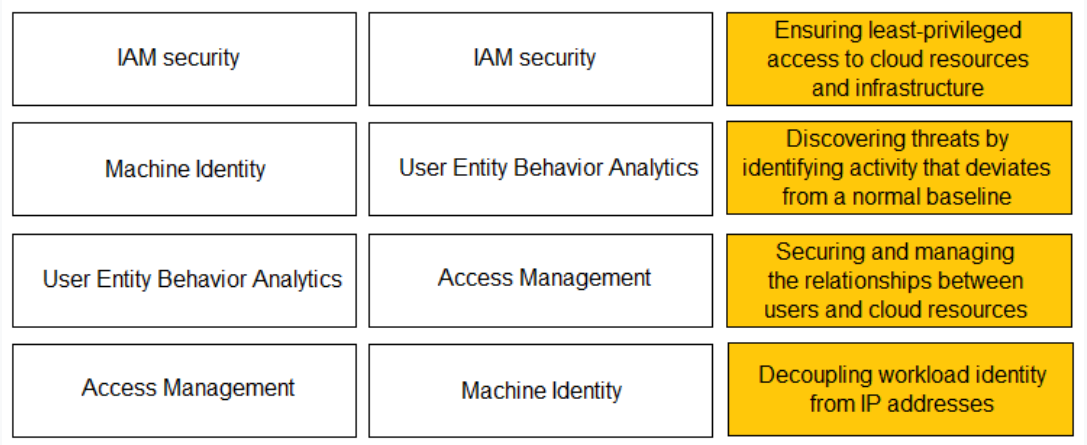
Match the Identity and Access Management (IAM) security control with the appropriate definition.

Select and Place:



Suggested Answer:





[Removed] Highly Voted 3 years, 7 months ago

Flip Access managment & IAM Key capabilities include: ● Identity and Access Management (IAM) security: Secure and manage the relationships between users and cloud resources. Enforce governance policies to ensure that users and resources behave only as intended and do not introduce risk to the environment. ● Access management: Ensure least-privileged access to cloud resources and infrastructure, and decouple user permissions from workload permissions. ● Machine identity: Decouple workload identity from IP addresses. Leverage tags and metadata to assign a logical identity to applications and workloads, and then use it to enforce ID-based micro-segmentation and security policies that adapt to your dynamic environments. ● UEBA: Continuously analyze the behavior of users and resources in your cloud to detect and prevent anomalous behavior,

such as an admin logging in from an unknown location or a container accessing a file it should not be able to access.Correct. Found on Page 149 of the study guide.

upvoted 10 times

[Removed] Highly Voted 3 years, 7 months ago

Flip Access managment & IAM

Key capabilities include: ● Identity and Access Management (IAM) security: Secure and manage the relationships between users and cloud resources. Enforce governance policies to ensure that users and resources behave only as intended and do not introduce risk to the environment. ● Access management: Ensure least-privileged access to cloud resources and infrastructure, and decouple user permissions from workload permissions. ● Machine identity: Decouple workload identity from IP addresses. Leverage tags and metadata to assign a logical identity to applications and workloads, and then use it to enforce ID-based micro-segmentation and security policies that adapt to your dynamic environments. ● UEBA: Continuously analyze the behavior of users and resources in your cloud to detect and prevent anomalous behavior, such as an admin logging in from an unknown location or a container accessing a file it should not be able to access.

upvoted 10 times

David9385738 Most Recent 1 year, 9 months ago

Correct. Found on Page 149 of the study guide.

upvoted 1 times

Question #8 *Topic 1*

On an endpoint, which method should you use to secure applications against exploits?

A. endpoint-based firewall

B. strong user passwords

C. full-disk encryption

D. software patches

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

blahblah1234567890000 Highly Voted 3 years, 5 months ago

I am not so sure that A i9s the correct answer, I think its D:

New software vulnerabilities and exploits are discovered all the time and thus diligent software patch management is required by system and security administrators in every organization.

upvoted 7 times

blahblah1234567890000 Highly Voted 3 years, 5 months ago

I am not so sure that A i9s the correct answer, I think its D: New software vulnerabilities and exploits are discovered all the time and thus diligent software patch management is required by system and security administrators in every organization.I agree, what are you going to do with the endpoint firewall, block the application from working? No, you are going to patch the software to allow it to work and then not be vulnerable anymore.

upvoted 7 times

duckduckgooo 3 years, 4 months ago

I agree, what are you going to do with the endpoint firewall, block the application from working? No, you are going to patch the software to allow it to work and then not be vulnerable anymore.

upvoted 2 times

emlee Most Recent 1 year, 11 months ago

software patches

upvoted 2 times

Amaury93 3 years, 2 months ago

it should be software patches

upvoted 4 times

Question #9 *Topic 1*

Which not-for-profit organization maintains the common vulnerability exposure catalog that is available through their public website?

A. Department of Homeland Security

B. MITRE

C. Office of Cyber Security and Information Assurance

D. Cybersecurity Vulnerability Research Center

Suggested Answer: *B*
Official Answer: B

Currently there are no comments in this discussion, be the first to comment!

Question #10 *Topic 1*

Which Palo Alto Networks tools enable a proactive, prevention-based approach to network automation that accelerates security analysis?

A. MineMeld

B. AutoFocus

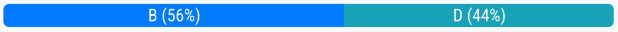
C. WildFire

D. Cortex XDR

Suggested Answer: *B*

Official Answer: B

Community vote distribution



rob899 Most Recent 3 years, 5 months ago

From the Practice Test on the official beacon site of palo alto the answer is AutoFocus. B

upvoted 1 times

blahblah1234567890000 4 years, 1 month ago

Page 252 "Palo Alto Networks AutoFocus enables a proactive, prevention-based approach to network security that puts automation to work for security professionals. Threat intelligence from the service is made directly accessible in the Palo Alto Networks platform, including PAN-OS software and Panorama. AutoFocus speeds the security team's existing workflows, which allows for in-depth investigation into suspicious activity, without additional specialized resources."could also be cortex based on a google search, idk wtf.

upvoted 3 times

blahblah1234567890000 4 years, 1 month ago

Selected Answer: B

Page 252 "Palo Alto Networks AutoFocus enables a proactive, prevention-based approach to network security that puts automation to work for security professionals. Threat intelligence from the service is made directly accessible in the Palo Alto Networks platform, including PAN-OS software and Panorama. AutoFocus speeds the security team's existing workflows, which allows for in-depth investigation into suspicious activity, without additional specialized resources."

upvoted 3 times

blahblah1234567890000 4 years, 1 month ago

could also be cortex based on a google search, idk wtf.

upvoted 1 times

Merlin0o 4 years, 2 months ago

Should be: Cortex XDR https://www.paloaltonetworks.com/cyberpedia/what-is-xdr "XDR solutions bring a proactive approach to threat detection and response. It delivers visibility across all data, including endpoint, network, and cloud data, while applying analytics and automation to address today's increasingly sophisticated threats."

upvoted 4 times

error_909 4 years, 5 months ago

answer is auto focus

upvoted 2 times

Question #11 *Topic 1*

Which endpoint product from Palo Alto Networks can help with SOC visibility?

A. STIX

B. Cortex XDR

C. WildFire

D. AutoFocus

Suggested Answer: *B*

Official Answer: B

Community vote distribution

B (100%)

blahblah1234567890000 1 year, 12 months ago

Pg.251Fat fingered the pg #217. XDR solutions bring a proactive approach to threat detection and response. It delivers visibility across all data, including endpoint, network, and cloud data, while applying analytics and automation to address today's increasingly sophisticated threats. With XDR, cybersecurity teams can: ● Identify hidden, stealthy, and sophisticated threats proactively and quickly ● Track threats across any source or location within the organization ● Increase the productivity of the people operating the technology ● Get more out of their security investments ● Conclude investigations more efficiently

upvoted 1 times

blahblah1234567890000 1 year, 12 months ago

Selected Answer: B

Pg.251

upvoted 1 times

blahblah1234567890000 Most Recent 1 year, 11 months ago

Fat fingered the pg #217. XDR solutions bring a proactive approach to threat detection and response. It delivers visibility across all data, including endpoint, network, and cloud data, while applying analytics and automation to address today's increasingly sophisticated threats. With XDR, cybersecurity teams can: ● Identify hidden, stealthy, and sophisticated threats proactively and quickly ● Track threats across any source or location within the organization ● Increase the productivity of the people operating the technology ● Get more out of their security investments ● Conclude investigations more efficiently

upvoted 2 times

Question #12 *Topic 1*

Which technique changes protocols at random during a session?

A. use of non-standard ports

B. port hopping

C. hiding within SSL encryption

D. tunneling within commonly used services

Suggested Answer: *B*

Official Answer: B

Community vote distribution

B (100%)

blahblah1234567890000 2 years, 1 month ago

Selected Answer: B

answer is b

upvoted 1 times

blahblah1234567890000 2 years, 1 month ago

answer is bPort hopping, in which ports and protocols are randomly changed during a session.

upvoted 1 times

blahblah1234567890000 **Most Recent** 1 year, 11 months ago

Port hopping, in which ports and protocols are randomly changed during a session.

upvoted 3 times

Question #13 *Topic 1*

What is the primary security focus after consolidating data center hypervisor hosts within trust levels?

A. control and protect inter-host traffic using routers configured to use the Border Gateway Protocol (BGP) dynamic routing protocol

B. control and protect inter-host traffic by exporting all your traffic logs to a sysvol log server using the User Datagram Protocol (UDP)

C. control and protect inter-host traffic by using IPv4 addressing

D. control and protect inter-host traffic using physical network security appliances

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

blahblah1234567890000 Most Recent 2 years, 1 month ago

page 211 "Consolidating servers within trust levels: Organizations often consolidate servers within the same trust level into a single virtual computing environment: ... ... This virtual systems capability enables a single physical device to be used to simultaneously meet the unique requirements of multiple VMs or groups of VMs. Control and protection of inter-host traffic with physical network security appliances that are properly positioned and configured is the primary security focus."

upvoted 3 times

Question #14 *Topic 1*

Which product from Palo Alto Networks extends the Security Operating Platform with the global threat intelligence and attack context needed to accelerate analysis, forensics, and hunting workflows?

A. Global Protect

B. WildFire

C. AutoFocus

D. STIX

Suggested Answer: *C*

Official Answer: C

Community vote distribution

C (100%)

blahblah1234567890000 Most Recent 2 years, 1 month ago

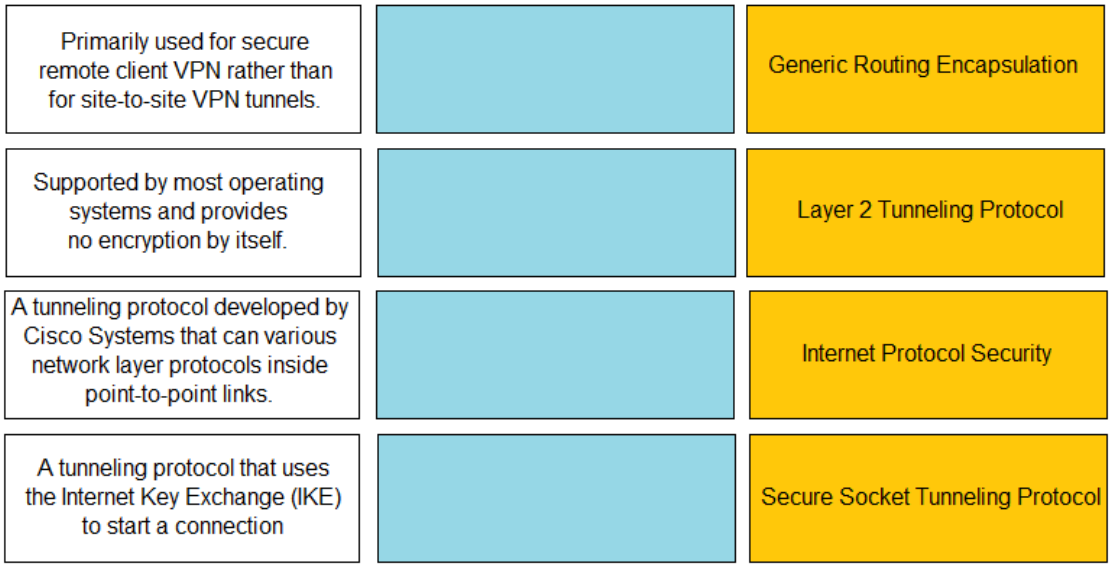
page 173 "AutoFocus makes over a billion samples and sessions, including billions of artifacts, immediately actionable for security analysis and response efforts. AutoFocus extends the product portfolio with the global threat intelligence and attack context needed to accelerate analysis, forensics, and hunting workflows. Together, the platform and AutoFocus move security teams away from legacy manual approaches that rely on aggregating a growing number of detectionbased alerts and post-event mitigation, to preventing sophisticated attacks and enabling proactive hunting activities."

upvoted 1 times

DRAG DROP -

Match the description with the VPN technology.

Select and Place:



Suggested Answer:

Primarily used for secure remote client VPN rather than for site-to-site VPN tunnels.	A tunneling protocol developed by Cisco Systems that can various network layer protocols inside point-to-point links.	Generic Routing Encapsulation
Supported by most operating systems and provides no encryption by itself.	Supported by most operating systems and provides no encryption by itself.	Layer 2 Tunneling Protocol
A tunneling protocol developed by Cisco Systems that can various network layer protocols inside point-to-point links.	A tunneling protocol that uses the Internet Key Exchange (IKE) to start a connection	Internet Protocol Security
A tunneling protocol that uses the Internet Key Exchange (IKE) to start a connection	Primarily used for secure remote client VPN rather than for site-to-site VPN tunnels.	Secure Socket Tunneling Protocol

Primarily used for secure remote client VPN rather than for site-to-site VPN tunnels.	A tunneling protocol developed by Cisco Systems that can various network layer protocols inside point-to-point links.	Generic Routing Encapsulation
Supported by most operating systems and provides no encryption by itself.	Supported by most operating systems and provides no encryption by itself.	Layer 2 Tunneling Protocol
A tunneling protocol developed by Cisco Systems that can various network layer protocols inside point-to-point links.	A tunneling protocol that uses the Internet Key Exchange (IKE) to start a connection	Internet Protocol Security
A tunneling protocol that uses the Internet Key Exchange (IKE) to start a connection	Primarily used for secure remote client VPN rather than for site-to-site VPN tunnels.	Secure Socket Tunneling Protocol

blahblah1234567890000 Most Recent 1 year, 11 months ago

The answers here are correct in the question.

upvoted 1 times

blahblah1234567890000 1 year, 11 months ago

Layer 2 Tunneling Protocol: Layer 2 Tunneling Protocol (L2TP) is supported by most operating systems (including mobile devices). Although it provides no encryption by itself, it is considered secure when used together with IPsec. Secure Socket Tunneling Protocol: Secure Socket Tunneling Protocol (SSTP) is a VPN tunnel created by Microsoft to transport PPP or L2TP traffic through an SSL 3.0 channel. SSTP primarily is used for secure remote client VPN access, rather than for site-to-site VPN tunnels. Microsoft Point-to-Point Encryption: Microsoft Point-to-Point Encryption (MPPE) encrypts data in PPP-based dial-up connections or PPTP VPN connections. MPPE uses the RSA RC4 encryption algOpenVPN: OpenVPN is a highly secure, open-source VPN implementation that uses SSL/TLS encryption for key exchange. OpenVPN uses up to 256-bit encryption and can run over TCP or UDP. Although it is not natively supported by most major operating systems, it has been ported to most major operating systems, including mobile device operating systems.Internet Protocol Security: IPsec is a secure communications protocol that authenticates and encrypts IP packets in a communication session. An IPsec VPN requires compatible VPN client software to be installed on the endpoint device. A group password or key is required for configuration. Client-server IPsec VPNs typically require user action to initiate the connection, such as launching the client software and logging in with a username and password. A security association (SA) in IPsec defines how two or more entities will securely communicate over the network using IPsec. A single Internet Key Exchange (IKE) SA is established between communicating entities to initiate the IPsec VPN tunnel. Separate IPsec SAs are then established for each communication direction in a VPN session. An IPsec VPN can be configured to force all of the user's internet traffic back through an organization's firewall, thus providing optimal protection with enterprise-gra

upvoted 1 times

blahblah1234567890000 1 year, 11 months ago

Layer 2 Tunneling Protocol: Layer 2 Tunneling Protocol (L2TP) is supported by most operating systems (including mobile devices). Although it provides no encryption by itself, it is considered secure when used together with IPsec.

Secure Socket Tunneling Protocol: Secure Socket Tunneling Protocol (SSTP) is a VPN tunnel created by Microsoft to transport PPP or L2TP traffic through an SSL 3.0 channel. SSTP primarily is used for secure remote client VPN access, rather than for site-to-site VPN tunnels.

Microsoft Point-to-Point Encryption: Microsoft Point-to-Point Encryption (MPPE) encrypts data in PPP-based dial-up connections or PPTP VPN connections. MPPE uses the RSA RC4 encryption alg

upvoted 1 times

blahblah1234567890000 1 year, 11 months ago

OpenVPN: OpenVPN is a highly secure, open-source VPN implementation that uses SSL/TLS encryption for key exchange. OpenVPN uses up to 256-bit encryption and can run over TCP or UDP. Although it is not natively supported by most major operating systems, it has been ported to most major operating systems, including mobile device operating systems.

upvoted 1 times

blahblah1234567890000 1 year, 11 months ago

OpenVPN: OpenVPN is a highly secure, open-source VPN implementation that uses SSL/TLS encryption for key exchange. OpenVPN uses up to 256-bit encryption and can run over TCP or UDP. Although it is not natively supported by most major operating systems, it has been ported to most major operating systems, including mobile device operating systems.Internet Protocol Security: IPsec is a secure communications protocol that authenticates and encrypts IP packets in a communication session. An IPsec VPN requires compatible VPN client software to be installed on the endpoint device. A group password or key is required for configuration. Client-server IPsec VPNs typically require user action to initiate the connection, such as launching the client software and logging in with a username and password. A security association (SA) in IPsec defines how two or more entities will securely communicate over the network using IPsec. A single Internet Key Exchange (IKE) SA is established between communicating entities to initiate the IPsec VPN tunnel. Separate IPsec SAs are then established for each communication direction in a VPN session. An IPsec VPN can be configured to force all of the user's internet traffic back through an organization's firewall, thus providing optimal protection with enterprise-grade security but with some performance loss. Or split tunneling can be configured to allow internet traffic from the device to go directly to the internet, while other specific types of traffic route through the IPsec tunnel, for acceptable protection with much less performance degradation.Secure Sockets Layer: Secure Sockets Layer (SSL) is an asymmetric encryption protocol used to secure communication sessions. SSL has been superseded by Transport Layer Security (TLS), although SSL still is the more commonly used terminology. An SSL VPN can be deployed as an agent-based or agentless browser-based connection. An agentless SSL VPN requires users only to launch a web browser, open a VPN

upvoted 1 times

blahblah1234567890000 1 year, 11 months ago

Internet Protocol Security: IPsec is a secure communications protocol that authenticates and encrypts IP packets in a communication session. An IPsec VPN requires compatible VPN client software to be installed on the endpoint device. A group password or key is required for configuration. Client-server IPsec VPNs typically require user action to initiate the connection, such as launching the client software and logging in with a username and password. A security association (SA) in IPsec defines how two or more entities will securely communicate over the network using IPsec. A single Internet Key Exchange (IKE) SA is established between communicating entities to initiate the IPsec VPN tunnel. Separate IPsec SAs are then established for each communication direction in a VPN session. An IPsec VPN can be configured to force all of the user's internet traffic back through an organization's firewall, thus providing optimal protection with enterprise-grade security but with some performance loss. Or split tunneling can be configured to allow internet traffic from the device to go directly to the internet, while other specific types of traffic route through the IPsec tunnel, for acceptable protection with much less performance degradation.Secure Sockets Layer: Secure Sockets Layer (SSL) is an asymmetric encryption protocol used to secure communication sessions. SSL has been superseded by Transport Layer Security (TLS), although SSL still is the more commonly used terminology. An SSL VPN can be deployed as an agent-based or agentless browser-based connection. An agentless SSL VPN requires users only to launch a web browser, open a VPN portal or webpage using the HTTPS protocol, and log in to the network with their user credentials. An agent-based SSL client is used within the browser session, which persists only while the connection is active and removes itself when the connection is closed. This type of VPN can be particularly useful for remote users that are connecting fro

upvoted 1 times

blahblah1234567890000 1 year, 11 months ago

Internet Protocol Security: IPsec is a secure communications protocol that authenticates and encrypts IP packets in a communication session. An IPsec VPN requires compatible VPN client software to be installed on the endpoint device. A group password or key is required for configuration. Client-server IPsec VPNs typically require user action to initiate the connection, such as launching the client software and logging in with a username and password. A security association (SA) in IPsec defines how two or more entities will securely communicate over the network using IPsec. A single Internet Key Exchange (IKE) SA is established between communicating entities to initiate the IPsec VPN tunnel. Separate IPsec SAs are then established for each communication direction in a VPN session. An IPsec VPN can be configured to force all of the user's internet traffic back through an organization's firewall, thus providing optimal protection with enterprise-grade security but with some performance loss. Or split tunneling can be

configured to allow internet traffic from the device to go directly to the internet, while other specific types of traffic route through the IPsec tunnel, for acceptable protection with much less performance degradation.

upvoted 1 times

blahblah1234567890000 1 year, 11 months ago

Secure Sockets Layer: Secure Sockets Layer (SSL) is an asymmetric encryption protocol used to secure communication sessions. SSL has been superseded by Transport Layer Security (TLS), although SSL still is the more commonly used terminology. An SSL VPN can be deployed as an agent-based or agentless browser-based connection. An agentless SSL VPN requires users only to launch a web browser, open a VPN portal or webpage using the HTTPS protocol, and log in to the network with their user credentials. An agent-based SSL client is used within the browser session, which persists only while the connection is active and removes itself when the connection is closed. This type of VPN can be particularly useful for remote users that are connecting from an endpoint device they do not own or control, such as a hotel kiosk, where full client VPN software cannot be installed. SSL VPN technology has become the de facto standard and preferred method of connecting remote endpoint devices back to the enterprise network, and IPsec is most commonly used in site-to-site or device-to-device VPN connections, such as connecting a branch office network to a headquarters location network or data center.

upvoted 1 times

Question #16 *Topic 1*

Which characteristic of serverless computing enables developers to quickly deploy application code?

A. Uploading cloud service autoscaling services to deploy more virtual machines to run their application code based on user demand

B. Uploading the application code itself, without having to provision a full container image or any OS virtual machine components

C. Using cloud service spot pricing to reduce the cost of using virtual machines to run their application code

D. Using Container as a Service (CaaS) to deploy application containers to run their code.

Suggested Answer: *B*
Official Answer: B

Community vote distribution
B (100%)

Praveen33 Most Recent 1 year, 8 months ago
In serverless apps, the developer uploads only the app package itself, without a full container image or any OS components. The platform dynamically packages it into an image, runs the image in a container, and then (if needed) instantiates the underlying host OS and VM and the hardware required to run them. In a serverless model, users make the most dramatic trade-offs of compatibility and control for the simplest, most efficient deployment and management experience.
upvoted 1 times

rob899 2 years, 11 months ago
Answer is B from Official Practice test...
upvoted 1 times

Amaury93 3 years, 2 months ago
Answer is B. Page 167 of the stufy guide.*Study Guide
upvoted 1 times

Amaury93 3 years, 2 months ago
Selected Answer: B
Answer is B. Page 167 of the stufy guide.
upvoted 1 times

Amaury93 3 years, 2 months ago
*Study Guide
upvoted 1 times

maboom 3 years, 3 months ago
The answer is B
upvoted 1 times

handyplazt 3 years, 7 months ago
Answer is B From study guide "In serverless apps, the developer uploads only the app package itself, without a full container image or any OS components. The platform dynamically packages it into an image, runs the image in a container, and (if needed) instantiates the underlying host OS and VM and the hardware required to run them."
upvoted 1 times

error_909 3 years, 11 months ago
Answer is B
upvoted 2 times

Bubu3k 4 years ago
It's B
upvoted 2 times

Question #17 *Topic 1*

Which key component is used to configure a static route?

A. router ID

B. enable setting

C. routing protocol

D. next hop IP address

Suggested Answer: *D*
Official Answer: D

duckduckgooo Most Recent 1 year, 10 months ago

D https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/networking/static-routes/configure-a-static-route For Next Hop, select one of the following: IP Address—Enter the IP address (for example, 192.168.56.1 or 2001:db8:49e:1::1) when you want to route to a specific next hop. You must Enable IPv6 on the interface (when you Configure Layer 3 Interfaces) to use an IPv6 next hop address. If you're creating a default route, for Next Hop you must select IP Address and enter the IP address for your Internet gateway (for example, 192.168.56.1 or 2001:db8:49e:1::1). Alternatively, you can create an address object of type IP Netmask. The address object must have a netmask of /32 for IPv4 or /128 for IPv6.

upvoted 1 times

Question #18 *Topic 1*

A native hypervisor runs:

A. with extreme demands on network throughput

B. only on certain platforms

C. within an operating system's environment

D. directly on the host computer's hardware

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

blahblah1234567890000 Most Recent 1 year, 11 months ago

● Type 1 (native or bare metal). Runs directly on the host computer's hardware ● Type 2 (hosted). Runs within an operating system environment

upvoted 1 times

Merlin0o 2 years ago

D is correct: Page 296 of the study guide native hypervisor: A hypervisor that runs directly on the host computer hardware. Also known as a Type 1 or bare-metal hypervisor.

upvoted 1 times

Question #19 *Topic 1*

Which Palo Alto Networks product provides playbooks with 300+ multivendor integrations that help solve any security use case?

A. Cortex XSOAR

B. Prisma Cloud

C. AutoFocus

D. Cortex XDR

Suggested Answer: *A*

Official Answer: A

Community vote distribution

A (100%)

blahblah1234567890000 Most Recent 1 year, 11 months ago

SOAR tools ingest aggregated alerts from detection sources (such as SIEMs, network security tools, and mailboxes) before executing automatable, process-driven playbooks to enrich and respond to these alerts.

upvoted 2 times

error_909 2 years, 5 months ago

Answer is correcthttps://www.paloaltonetworks.com/cortex/security-operations-automation

upvoted 1 times

error_909 2 years, 5 months ago

Selected Answer: A

Answer is correct

upvoted 1 times

error_909 2 years, 5 months ago

https://www.paloaltonetworks.com/cortex/security-operations-automation

upvoted 1 times

Question #20 *Topic 1*

Which activities do local organization security policies cover for a SaaS application?

A. how the data is backed up in one or more locations

B. how the application can be used

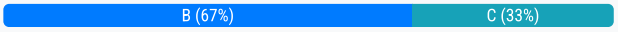
C. how the application processes the data

D. how the application can transit the Internet

Suggested Answer: *B*

Official Answer: B

Community vote distribution



f5d9c90 Most Recent 1 year, 8 months ago

he correct answer is: B. How the application can be used Explanation: Local organization security policies for a SaaS (Software as a Service) application typically define guidelines and rules for how employees or users within the organization can use the application. These policies address: Acceptable use of the application Access control and user permissions Data sharing and privacy rules Compliance requirements for the organization's data handling Security measures like password policies and multi-factor authentication (MFA)

upvoted 1 times

vriper 1 year, 11 months ago

B. how the application can be used The local organisation's security policies for a SaaS application typically cover how the application can be used. This includes guidelines on access, configuration and proper use of the application to ensure that security and compliance with organisational standards are maintained. Option C. how the application processes the data is also relevant, as security policies may include how information is handled and processed within the application to ensure data protection and regulatory compliance. However, in the context of organisational security policies for SaaS applications, it is more common to focus on how the application can be used (option B), as this covers practical aspects of access and use of the application by users, and policies usually define the rules for secure use of the application. Both options are important in the context of security, but option B is more directly applicable to usage policies within an organisation.

upvoted 1 times

mkucuk89 2 years, 7 months ago

Data security

upvoted 1 times

Question #21 *Topic 1*

Which Palo Alto Networks subscription service complements App-ID by enabling you to configure the next-generation firewall to identify and control access to websites and to protect your organization from websites hosting malware and phishing pages?

A. Threat Prevention

B. DNS Security

C. WildFire

D. URL Filtering

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

blahblah1234567890000 Most Recent 2 years ago

Pg.169 The URL Filtering service complements App-ID by enabling you to configure the next-generation firewall to identify and control access to websites and to protect your organization from websites that host malware and phishing pages.

upvoted 1 times

Question #22 *Topic 1*

Which option would be an example of PII that you need to prevent from leaving your enterprise network?

A. Credit card number

B. Trade secret

C. National security information

D. A symmetric encryption key

Suggested Answer: *A*
Official Answer: A

Currently there are no comments in this discussion, be the first to comment!

Question #23 *Topic 1*

Which network analysis tool can be used to record packet captures?

A. Smart IP Scanner

B. Wireshark

C. Angry IP Scanner

D. Netman

Suggested Answer: *B*
Official Answer: B

Currently there are no comments in this discussion, be the first to comment!

Question #24 *Topic 1*

Systems that allow for accelerated incident response through the execution of standardized and automated playbooks that work upon inputs from security technology and other data flows are known as what?

A. XDR

B. STEP

C. SOAR

D. SIEM

Suggested Answer: *C*

Official Answer: C

Community vote distribution

C (100%)

error_909 Most Recent 1 year, 11 months ago

https://www.paloaltonetworks.com/cortex/security-operations-automation

upvoted 2 times

Question #25 *Topic 1*

Which Palo Alto Networks tool is used to prevent endpoint systems from running malware executables such as viruses, trojans, and rootkits?

A. Expedition

B. Cortex XDR

C. AutoFocus

D. App-ID

Suggested Answer: *B*
Official Answer: B

Currently there are no comments in this discussion, be the first to comment!

Question #26 *Topic 1*

What does SIEM stand for?

A. Security Infosec and Event Management

B. Security Information and Event Management

C. Standard Installation and Event Media

D. Secure Infrastructure and Event Monitoring

Suggested Answer: *B*

Official Answer: B

Community vote distribution

B (100%)

blahblah1234567890000 Most Recent 1 year, 11 months ago

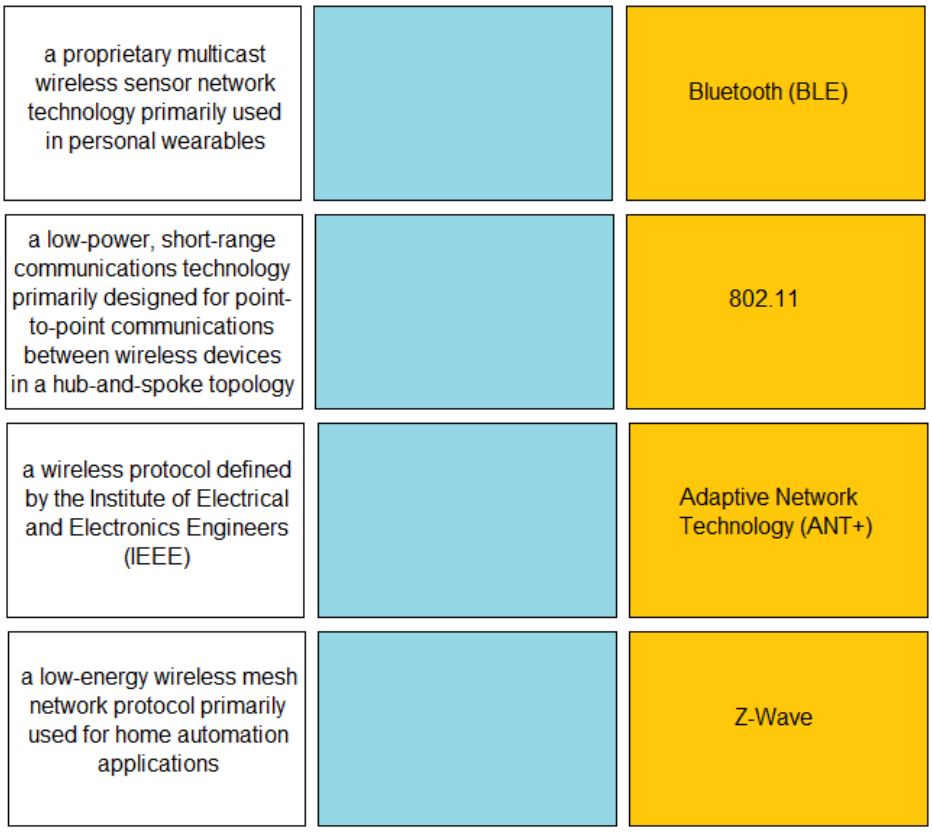
Originally designed as a tool to assist organizations with compliance and industry-specific regulations, security information and event management (SIEM) is a technology that has been around for almost two decades

upvoted 2 times

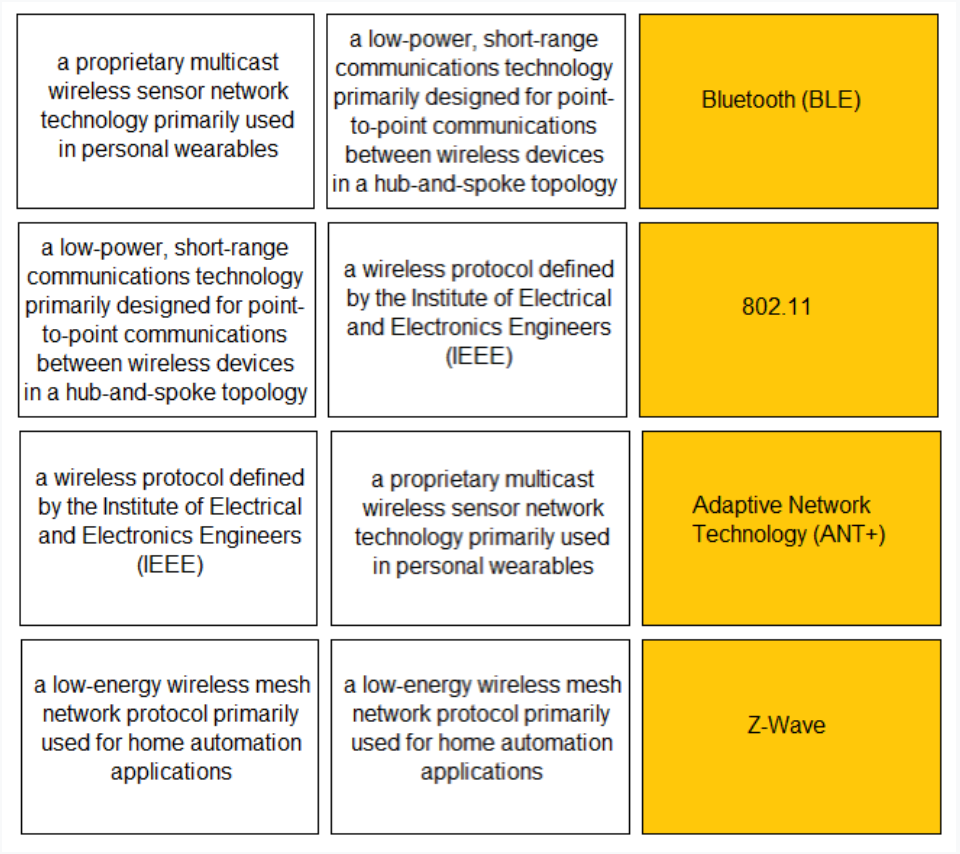
DRAG DROP -

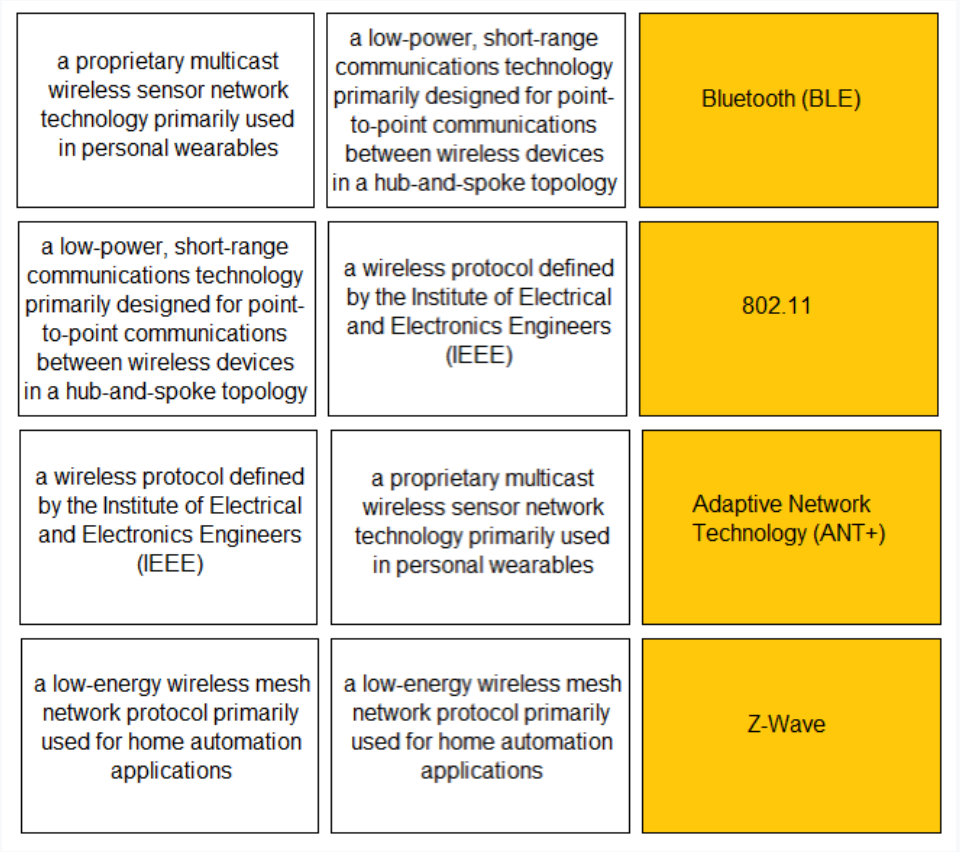
Match the IoT connectivity description with the technology.

Select and Place:



Suggested Answer:





blahblah1234567890000 Most Recent 1 year, 11 months ago

The answers here are correct.

upvoted 2 times

blahblah1234567890000 1 year, 11 months ago

Short-range wireless: ● Adaptive Network Technology+ (ANT+): ANT+ is a proprietary multicast wireless sensor network technology primarily used in personal wearables, such as sports and fitness sensors. ● Bluetooth/Bluetooth Low-Energy (BLE): Bluetooth is a low-power, short-range communications technology primarily designed for point-to-point communications between wireless devices in a hub-and-spoke topology. BLE (also known as Bluetooth Smart or Bluetooth 4.0+) devices consume significantly less power than Bluetooth devices and can access the internet directly through 6LoWPAN connectivity.● Internet Protocol version 6 (IPv6) over Low-Power Wireless Personal Area Networks (6LoWPAN): 6LoWPAN allows IPv6 traffic to be carried over low-power wireless mesh networks. 6LoWPAN is designed for nodes and applications that require wireless internet connectivity at relatively low data rates in small form factors, such as smart light bulbs and smart meters. ● Wi-Fi/802.11: The Institute of Electrical and Electronics Engineers (IEEE) defines the 802 LAN protocol standards. 802.11 is the set of standards used for Wi-Fi networks typically operating in the 2.4GHz and 5GHz frequency bands. The most common implementations today include: — 802.11n (labeled Wi-Fi 4 by the Wi-Fi Alliance), which operates on both 2.4GHz and 5GHz bands at ranges from 54Mbps to 600Mbps — 802.11ac (Wi-Fi 5), which operates on the 5GHz band at ranges from 433Mbps to 3.46 Gbps — 802.11ax (Wi-Fi 6), which operates on the 2.4GHz and 5GHz bands (and all bands between 1 and 6GHz, when they become available for 802.11 use) at ranges up to 11Gbps● Z-Wave: Z-Wave is a low-energy wireless mesh network protocol primarily used for home automation applications such as smart appliances, lighting control, security systems, smart thermostats, windows and locks, and garage doors. ● Zigbee/802.14: Zigbee is a low-cost, low-power wireless mesh network protocol based on the IEEE 802.15.4 standard. Zigbee is the dominant protoc

upvoted 1 times

blahblah1234567890000 1 year, 11 months ago

Short-range wireless: ● Adaptive Network Technology+ (ANT+): ANT+ is a proprietary multicast wireless sensor network technology primarily used in personal wearables, such as sports and fitness sensors. ● Bluetooth/Bluetooth Low-Energy (BLE): Bluetooth is a low-power, short-range communications technology primarily designed for point-to-point communications between wireless devices in a hub-and-spoke topology. BLE (also known as Bluetooth Smart or Bluetooth 4.0+) devices consume significantly less power than Bluetooth devices and can access the internet directly through 6LoWPAN connectivity.

upvoted 1 times

blahblah1234567890000 1 year, 11 months ago

● Internet Protocol version 6 (IPv6) over Low-Power Wireless Personal Area Networks (6LoWPAN): 6LoWPAN allows IPv6 traffic to be carried over low-power wireless mesh networks. 6LoWPAN is designed for nodes and applications that require wireless internet connectivity at relatively low data rates in small form factors, such as smart light bulbs and smart meters. ● Wi-Fi/802.11: The Institute of Electrical and Electronics Engineers (IEEE) defines the 802 LAN protocol standards. 802.11 is the set of standards used for Wi-Fi networks typically operating in the 2.4GHz and 5GHz frequency bands. The most common implementations today include: — 802.11n (labeled Wi-Fi 4 by the Wi-Fi Alliance), which operates on both 2.4GHz and 5GHz bands at ranges from 54Mbps to 600Mbps — 802.11ac (Wi-Fi 5), which operates on the 5GHz band at ranges from 433Mbps to 3.46 Gbps — 802.11ax (Wi-Fi 6), which operates on the 2.4GHz and 5GHz bands (and all bands between 1 and 6GHz, when they become available for 802.11 use) at ranges up to 11Gbps

upvoted 1 times

blahblah1234567890000 1 year, 11 months ago

● Internet Protocol version 6 (IPv6) over Low-Power Wireless Personal Area Networks (6LoWPAN): 6LoWPAN allows IPv6 traffic to be carried over low-power wireless mesh networks. 6LoWPAN is designed for nodes and applications that require wireless internet connectivity at relatively low data rates in small form factors, such as smart light bulbs and smart meters. ● Wi-Fi/802.11: The Institute of Electrical and Electronics Engineers (IEEE) defines the 802 LAN protocol standards. 802.11 is the set of standards used for Wi-Fi networks typically operating in the 2.4GHz and 5GHz frequency bands. The most common implementations today include: — 802.11n (labeled Wi-Fi 4 by the Wi-Fi Alliance), which operates on both 2.4GHz and 5GHz bands at ranges from 54Mbps to 600Mbps — 802.11ac (Wi-Fi 5), which operates on the 5GHz band at ranges from 433Mbps to 3.46 Gbps — 802.11ax (Wi-Fi 6), which operates on the 2.4GHz and 5GHz bands (and all bands between 1 and 6GHz, when they become available for 802.11 use) at ranges up to 11Gbps● Z-Wave: Z-Wave is a low-energy wireless mesh network protocol primarily used for home automation applications such as smart appliances, lighting control, security systems, smart thermostats, windows and locks, and garage doors. ● Zigbee/802.14: Zigbee is a low-cost, low-power wireless mesh network protocol based on the IEEE 802.15.4 standard. Zigbee is the dominant protocol in the low-power networking market, with a large installed base in industrial environments and smart home products.

upvoted 1 times

blahblah1234567890000 1 year, 11 months ago

● Z-Wave: Z-Wave is a low-energy wireless mesh network protocol primarily used for home automation applications such as smart appliances, lighting control, security systems, smart thermostats, windows and locks, and garage doors. ● Zigbee/802.14: Zigbee is a low-cost, low-power wireless mesh network protocol based on the IEEE 802.15.4 standard. Zigbee is the dominant protocol in the low-power networking market, with a large installed base in industrial environments and smart home products.

upvoted 1 times

Question #28 *Topic 1*

Which option is an example of a North-South traffic flow?

A. Lateral movement within a cloud or data center

B. An internal three-tier application

C. Client-server interactions that cross the edge perimeter

D. Traffic between an internal server and internal user

Suggested Answer: *C*

Official Answer: C

Community vote distribution

C (100%)

blahblah1234567890000 Most Recent 2 years ago

pg.208 North-south refers to data packets that move in and out of the virtualized environment from the host network or a corresponding traditional data center. North-south traffic is secured by one or more physical form factor perimeter edge firewalls.

upvoted 2 times

Question #29 *Topic 1*

Which aspect of a SaaS application requires compliance with local organizational security policies?

A. Types of physical storage media used

B. Data-at-rest encryption standards

C. Acceptable use of the SaaS application

D. Vulnerability scanning and management

Suggested Answer: *C*
Official Answer: C

Currently there are no comments in this discussion, be the first to comment!

Question #30 *Topic 1*

Which option describes the `selective network security virtualization` phase of incrementally transforming data centers?

A. during the selective network security virtualization phase, all intra-host communication paths are strictly controlled

B. during the selective network security virtualization phase, all intra-host traffic is forwarded to a Web proxy server

C. during the selective network security virtualization phase, all intra-host traffic is encapsulated and encrypted using the IPSEC protocol

D. during the selective network security virtualization phase, all intra-host traffic is load balanced

Suggested Answer: *A*

Official Answer: A

Community vote distribution

A (100%)

blahblah1234567890000 Most Recent 2 years ago

pg.212 Selective network security virtualization: Intra-host communications and live migrations are architected at this phase. All intra-host communication paths are strictly controlled to ensure that traffic between VMs at different trust levels is intermediated either by an on-box, virtual security appliance or by an off-box, physical security appliance.

upvoted 2 times

Question #31 *Topic 1*

Which TCP/IP sub-protocol operates at the Layer7 of the OSI model?

A. UDP

B. MAC

C. SNMP

D. NFS

Suggested Answer: *C*

Official Answer: C

Community vote distribution

C (100%)

fabeele Most Recent 1 year, 11 months ago

I go with D. SNMP: udp 161/162 NFS: TCP and udp 2049 The question specifies TCP!!

upvoted 1 times

kirmanis 1 year, 11 months ago

Correct answer is C. SNMP (Simple Network Management Protocol) is a TCP/IP sub-protocol that operates at the Application layer (Layer 7) of the OSI model. It's designed for network management, allowing network administrators to monitor and control network devices. NFS is an application-level protocol that operates at the Application layer (Layer 7) of the OSI model, but it's not specifically a TCP/IP sub-protocol.

upvoted 1 times

Robin997 1 year, 11 months ago

The correct answer is C. SNMP. Here's why: UDP (A) operates at the Transport Layer (Layer 4) of the OSI model, not at Layer 7. MAC (B) refers to the Media Access Control protocol, which operates at the Data Link Layer (Layer 2). SNMP (C), or Simple Network Management Protocol, is a protocol that operates at the Application Layer (Layer 7) for managing and monitoring network devices. NFS (D), or Network File System, also operates at Layer 7, but the question asks for a specific TCP/IP sub-protocol, and SNMP is more appropriate as it directly deals with network management.

upvoted 1 times

Robin997 1 year, 11 months ago

D. NFS The OSI model's Layer 7 is the Application Layer, where protocols related to specific network services operate. NFS (Network File System) is an application-layer protocol that allows file access over a network.

upvoted 1 times

Praveen33 2 years, 2 months ago

Correct answer : D

upvoted 1 times

blahblah1234567890000 3 years, 11 months ago

● Application (Layer 7 or L7): This layer identifies and establishes availability of communication partners, determines resource availability, and synchronizes communication. ● Presentation (Layer 6 or L6): This layer provides coding and conversion functions (such as data representation, character conversion, data compression, and data encryption) to ensure that data sent from the Application layer of one system is compatible with the Application layer of the receiving system. ● Session (Layer 5 or L5): This layer manages communication sessions (service requests and service responses) between networked systems, including connection establishment, data transfer, and connection release. ● Transport (Layer 4 or L4): This layer provides transparent, reliable data transport and end-to-end transmission control.● Network (Layer 3 or L3): This layer provides routing and related functions that enable data to be transported between systems on the same network or on interconnected networks. Routing protocols are defined at this layer. Logical addressing of devices on the network is accomplished at this layer using routed protocols such as Internet Protocol (IP). Routers operate at the Network layer of the OSI model. ● Data Link (Layer 2): This layer ensures that messages are delivered to the proper device across a physical network link. ● Physical (Layer 1 or L1): This layer sends and receives bits across the network medium (cabling or wireless links) from one device to another. It specifies the electrical, mechanical, and functional requirements of the network, including network topology, cabling and connectors, and interface types, and the process for converting bits to electrical (or light) signals that can be transmitted across the physical medium.

upvoted 4 times

blahblah1234567890000 3 years, 11 months ago

● Application (Layer 7 or L7): This layer identifies and establishes availability of communication partners, determines resource availability, and synchronizes communication. ● Presentation (Layer 6 or L6): This layer provides coding and conversion functions (such as data representation, character conversion, data compression, and data encryption) to ensure that data sent from the Application layer of one system is compatible with the Application layer of the receiving system. ● Session (Layer 5 or L5): This layer manages communication sessions (service requests and service responses) between networked systems, including connection establishment, data transfer, and connection release. ● Transport (Layer 4 or L4): This layer provides transparent, reliable data transport and end-to-end transmission control.

upvoted 4 times

blahblah1234567890000 3 years, 11 months ago

● Network (Layer 3 or L3): This layer provides routing and related functions that enable data to be transported between systems on the same network or on interconnected networks. Routing protocols are defined at this layer. Logical addressing of devices on the network is accomplished at this layer using routed protocols such as Internet Protocol (IP). Routers operate at the Network layer of the OSI model. ● Data Link (Layer 2): This layer ensures that messages are delivered to the proper device across a physical network link. ● Physical (Layer 1 or L1): This layer sends and receives bits across the network medium (cabling or wireless links) from one device to another. It specifies the electrical, mechanical, and functional requirements of the network, including network topology, cabling and connectors, and interface types, and the process for converting bits to electrical (or light) signals that can be transmitted across the physical medium.

upvoted 4 times

Question #32 *Topic 1*

Anthem server breaches disclosed Personally Identifiable Information (PII) from a number of its servers. The infiltration by hackers was attributed to which type of vulnerability?

A. an intranet-accessed contractor's system that was compromised

B. exploitation of an unpatched security vulnerability

C. access by using a third-party vendor's password

D. a phishing scheme that captured a database administrator's password

Suggested Answer: *D*
Official Answer: D

FC49 Most Recent 1 year, 10 months ago

Date: February 2015 Impact: Theft of up to 78.8 million current and former customers In February 2015, a single user at an Anthem subsidiary clicked on a phishing email which gave attackers access to:

upvoted 1 times

Question #33 *Topic 1*

Routing Information Protocol (RIP), uses what metric to determine how network traffic should flow?

A. Shortest Path

B. Hop Count

C. Split Horizon

D. Path Vector

Suggested Answer: *B*

Official Answer: B

Community vote distribution

B (100%)

blahblah1234567890000 Most Recent 1 year, 11 months ago

Routing Information Protocol (RIP) is an example of a distance-vector routing protocol that uses hop count as its routing metric. To prevent routing loops, in which packets effectively get stuck bouncing between various router nodes, RIP implements a hop limit of 15, which limits the size of networks that RIP can support. After a data packet crosses 15 router nodes (hops) between a source and a destination, the destination is considered unreachable.

upvoted 1 times

Question #34 *Topic 1*

Why is it important to protect East-West traffic within a private cloud?

A. All traffic contains threats, so enterprises must protect against threats across the entire network

B. East-West traffic contains more session-oriented traffic than other traffic

C. East-West traffic contains more threats than other traffic

D. East-West traffic uses IPv6 which is less secure than IPv4

Suggested Answer: *A*

Official Answer: A

Community vote distribution

A (100%)

kirmanis Most Recent 1 year, 11 months ago

While it's true that East-West traffic (traffic within a private cloud) might not be as exposed to external threats as North-South traffic (traffic between the private cloud and the internet), it's still crucial to protect it. Here's why: Internal threats: Even within a private cloud, there are risks of data breaches, unauthorized access, and other security incidents that can originate from internal sources. Data sensitivity: East-West traffic often involves sensitive data that needs to be protected from unauthorized access and disclosure. Compliance requirements: Many regulations and industry standards require organizations to implement strong security measures to protect their data, regardless of whether the traffic is internal or external.

upvoted 1 times

Question #35 *Topic 1*

Which IPsec feature allows device traffic to go directly to the Internet?

A. Split tunneling

B. Diffie-Hellman groups

C. d.Authentication Header (AH)

D. IKE Security Association

Suggested Answer: *A*

Official Answer: A

Community vote distribution

A (100%)

blahblah1234567890000 Most Recent 1 year, 11 months ago

"Or split tunneling can be configured to allow internet traffic from the device to go directly to the internet, while other specific types of traffic route through the IPsec tunnel, for acceptable protection with much less performance degradation."

upvoted 2 times

Question #36 *Topic 1*

Which attacker profile uses the internet to recruit members to an ideology, to train them, and to spread fear and include panic?

A. cybercriminals

B. state-affiliated groups

C. hacktivists

D. cyberterrorists

Suggested Answer: *D*
Official Answer: D

duckduckgooo Most Recent 1 year, 10 months ago

From Study guide Cyberterrorists: Terrorist organizations use the internet to recruit, train, instruct, and communicate, and to spread fear and panic to advance their ideologies. Unlike other threat actors, cyberterrorists are largely indiscriminate in their attacks, and their objectives include physical harm, death, and destruction.

upvoted 1 times

Question #37 *Topic 1*

What are two key characteristics of a Type 1 hypervisor? (Choose two.)

A. is hardened against cyber attacks

B. runs without any vulnerability issues

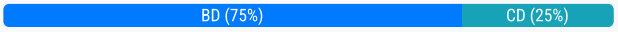
C. runs within an operating system

D. allows multiple, virtual (or guest) operating systems to run concurrently on a single physical host computer

Suggested Answer: *B, D*

Official Answer: BD

Community vote distribution



dax 2 years, 1 month ago

B and d are the correct answer. The most commonly deployed type of hypervisor is the type 1 or bare-metal hypervisor, where virtualization software is installed directly on the hardware where the operating system is normally installed. Because bare-metal hypervisors are isolated from the attack-prone operating system, they are extremely secure. C means hosted hypervisor or type 2

upvoted 1 times

dax 2 years, 1 month ago

C and d are correct. C is correct like hyper-V Unless it says run ON TOP of an OS which is type 2 hypervisor.Disregard

upvoted 1 times

dax 2 years, 1 month ago

C and d are correct. C is correct like hyper-V Unless it says run ON TOP of an OS which is type 2 hypervisor.

upvoted 1 times

dax Most Recent 2 years, 1 month ago

Disregard

upvoted 1 times

maboom 2 years, 3 months ago

The question is supposed to be about Type 2 hypervisors. This question is also in the PCCET Practice exam provided by Palo on Beacon.

upvoted 2 times

blahblah1234567890000 2 years, 6 months ago

I bet the question was supposed to ask about Type 2 hypervisors: The two types of hypervisors are: ● Type 1 (native or bare metal). Runs directly on the host computer's hardware ● Type 2 (hosted). Runs within an operating system environment

upvoted 3 times

Merlin0o 2 years, 6 months ago

Should be B and D Page 193 of the study guide: "● A hypervisor allows multiple, virtual (or guest) operating systems to run concurrently on a single physical host computer. ● A native (also known as a Type 1 or bare metal) hypervisor runs directly on the host computer's hardware. ● A hosted (also known as a Type 2) hypervisor runs within an operating system environment."

upvoted 3 times

error_909 2 years, 11 months ago

C; without instead of with

upvoted 1 times

Noraschid 3 years ago

Should be B and D.

upvoted 1 times

Pathfndr 3 years, 1 month ago

This answer is incorrect. It does not run within an operating system, it is installed on bare metal.

upvoted 3 times

Question #38 *Topic 1*

The customer is responsible only for which type of security when using a SaaS application?

A. physical

B. platform

C. data

D. infrastructure

Suggested Answer: *C*
Official Answer: C

Currently there are no comments in this discussion, be the first to comment!

Question #39 *Topic 1*

Which Palo Alto subscription service identifies unknown malware, zero-day exploits, and advanced persistent threats (APTs) through static and dynamic analysis in a scalable, virtual environment?

A. DNS Security

B. URL Filtering

C. WildFire

D. Threat Prevention

Suggested Answer: *C*

Official Answer: C

Community vote distribution

C (100%)

blahblah1234567890000 Most Recent 1 year, 11 months ago

"The WildFire cloud-based malware analysis environment is a cyber threat prevention service that identifies unknown malware, zero-day exploits, and advanced persistent threats (APTs) through static and dynamic analysis in a scalable, virtual environment. WildFire automatically disseminates updated protections in near-real time to immediately prevent threats from spreading; this occurs without manual intervention"

upvoted 3 times

Question #40 *Topic 1*

In which step of the cyber-attack lifecycle do hackers embed intruder code within seemingly innocuous files?

A. weaponization

B. reconnaissance

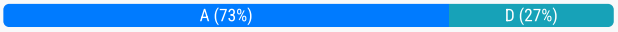
C. exploitation

D. delivery

Suggested Answer: *A*

Official Answer: A

Community vote distribution



kirmanis Most Recent 1 year, 11 months ago

Pg 31 PCCET Study Guide While it's true that East-West traffic (traffic within a private cloud) might not be as exposed to external threats as North-South traffic (traffic between the private cloud and the internet), it's still crucial to protect it. Here's why: Internal threats: Even within a private cloud, there are risks of data breaches, unauthorized access, and other security incidents that can originate from internal sources. Data sensitivity: East-West traffic often involves sensitive data that needs to be protected from unauthorized access and disclosure. Compliance requirements: Many regulations and industry standards require organizations to implement strong security measures to protect their data, regardless of whether the traffic is internal or external.

upvoted 1 times

csco10320953 3 years, 7 months ago

Weaponization -stage -Its only desire which type method to be identify Delivery -attach/insert the code/file So answer is :Delivery

upvoted 1 times

phil155 3 years, 11 months ago

"Weaponization: Next, attackers determine which methods to use to compromise a target endpoint. They may choose to embed intruder code within seemingly innocuous files such as a PDF or Microsoft Word document or email message."

upvoted 2 times

blahblah1234567890000 4 years ago

Weaponization

upvoted 2 times

Merlin0o 4 years ago

Should be A, Page 39 study guide. Weaponization: They may choose to embed intruder code within seemingly innocuous files such as a PDF or Microsoft Word document Delivery: Attackers next attempt to deliver their weaponized payload to a target endpoint

upvoted 3 times

n3etw0 4 years, 3 months ago

A - page 39 of study guide

upvoted 4 times

error_909 4 years, 5 months ago

Selected Answer: D

In weaponization, the hacker only identify the method, but in delivery it attach the hack to the innocent payload

upvoted 3 times

error_909 4 years, 5 months ago

In weaponization, the hacker only identify the method, but in delivery it attach the hack to the innocent payloadITS A Sorry

upvoted 3 times

error_909 4 years, 5 months ago

ITS A Sorry

upvoted 1 times

Question #41 *Topic 1*

Which endpoint tool or agent can enact behavior-based protection?

A. AutoFocus

B. Cortex XDR

C. DNS Security

D. MineMeld

Suggested Answer: *B*

Official Answer: B

Community vote distribution

B (100%)

blahblah1234567890000 Most Recent 1 year, 11 months ago

Its Cortex XDR

upvoted 2 times

jshow 3 years, 3 months ago

B is correct

upvoted 3 times

Question #42 *Topic 1*

Which tool supercharges security operations center (SOC) efficiency with the world's most comprehensive operating platform for enterprise security?

A. Prisma SAAS

B. WildFire

C. Cortex XDR

D. Cortex XSOAR

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

blahblah1234567890000 Most Recent 1 year, 11 months ago

Cortex XSOAR enhances Security Operations Center (SOC) efficiency with the world's most comprehensive operating platform for enterprise security. Cortex XSOAR unifies case management, automation, real-time collaboration, and native threat intel management in the industry's first extended security orchestration, automation, and response (SOAR) offering.

upvoted 3 times

Question #43 *Topic 1*

During the OSI layer 3 step of the encapsulation process, what is the Protocol Data Unit (PDU) called when the IP stack adds source (sender) and destination
(receiver) IP addresses?

A. Frame

B. Segment

C. Packet

D. Data

Suggested Answer: *C*
Official Answer: C

Community vote distribution
C (100%)

blahblah1234567890000 Most Recent 1 year, 11 months ago

The IP stack adds source (sender) and destination (receiver) IP addresses to the TCP segment (which now is called an IP packet) and notifies the server operating system that it has an outgoing message ready to be sent across the network.
upvoted 2 times

Question #44 *Topic 1*

Which core component is used to implement a Zero Trust architecture?

A. VPN Concentrator

B. Content Identification

C. Segmentation Platform

D. Web Application Zone

Suggested Answer: *C*

Official Answer: C

Community vote distribution

C (100%)

blahblah1234567890000 Most Recent 1 year, 11 months ago

"Remember that a trust zone is not intended to be a “pocket of trust” where systems (and therefore threats) within the zone can communicate freely and directly with each other. For a full Zero Trust implementation, the network would be configured to ensure that all communications traffic, including traffic between devices in the same zone, is intermediated by the corresponding Zero Trust Segmentation Platform."

upvoted 2 times

Question #45 *Topic 1*

In addition to local analysis, what can send unknown files to WildFire for discovery and deeper analysis to rapidly detect potentially unknown malware?

A. Cortex XDR

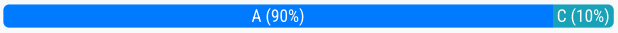
B. AutoFocus

C. MineMild

D. Cortex XSOAR

Suggested Answer: *A*
Official Answer: A

Community vote distribution



blahblah1234567890000 Most Recent 1 year, 11 months ago
Had to do some googling to find this information: In addition to local analysis, Cortex XDR can send unknown files to WildFire for discovery and deeper analysis to rapidly detect.
upvoted 3 times

error_909 2 years, 5 months ago
Answe is A
upvoted 3 times

RonJon 2 years, 5 months ago
Page 240 of the study guide In a ddition to local analysis, Cortex XDR can send unknown files to WildFire for discovery and deeper analysis to rapidly detect potentially unknown malware.
upvoted 3 times

error_909 2 years, 5 months ago
Selected Answer: C
AutoFocus contextual threat intelligence service speeds your ability to analyze threats and respond to cyberattacks. Instant access to community-based threat data from WildFire, enhanced with deep context and attribution from the Palo Alto Networks Unit 42 threat research team, saves time. Your security teams get detailed insight into attacks with prebuilt Unit 42 tags that identify malware families, adversaries, campaigns, malicious behaviors, and exploits without the need for a dedicated research team.
upvoted 1 times

error_909 2 years, 5 months ago
AutoFocus contextual threat intelligence service speeds your ability to analyze threats and respond to cyberattacks. Instant access to community-based threat data from WildFire, enhanced with deep context and attribution from the Palo Alto Networks Unit 42 threat research team, saves time. Your security teams get detailed insight into attacks with prebuilt Unit 42 tags that identify malware families, adversaries, campaigns, malicious behaviors, and exploits without the need for a dedicated research team.Sorry its Awrong again. its a. Why answer if you don't know the answers.
upvoted 1 times

error_909 2 years, 5 months ago
Sorry its A
upvoted 1 times

blahblah1234567890000 1 year, 11 months ago
wrong again. its a. Why answer if you don't know the answers.
upvoted 3 times

Question #46 *Topic 1*

On an endpoint, which method is used to protect proprietary data stored on a laptop that has been stolen?

A. operating system patches

B. full-disk encryption

C. periodic data backups

D. endpoint-based firewall

Suggested Answer: *B*
Official Answer: B

lookup Most Recent 1 year, 10 months ago

Yes, correct

upvoted 3 times

Question #47 *Topic 1*

Why have software developers widely embraced the use of containers?

A. Containers require separate development and production environments to promote authentic code.

B. Containers share application dependencies with other containers and with their host computer.

C. Containers simplify the building and deploying of cloud native applications.

D. Containers are host specific and are not portable across different virtual machine hosts.

Suggested Answer: *C*
Official Answer: C

Currently there are no comments in this discussion, be the first to comment!

Question #48 *Topic 1*

When signature-based antivirus software detects malware, what three things does it do to provide protection? (Choose three.)

A. decrypt the infected file using base64

B. alert system administrators

C. quarantine the infected file

D. delete the infected file

E. remove the infected file's extension

Suggested Answer: *B, C, D*

Official Answer: BCD

Community vote distribution

BCD (100%)

massyyy Highly Voted 3 years, 7 months ago

The response to this question is wrong. the right response : Quarantine: Isolates the infected file so that it cannot infect the endpoint or other files ● Delete: Removes the infected file ● Alert: Notifies the user (and/or system administrator) that malware has been detected

upvoted 7 times

error_909 Highly Voted 2 years, 11 months ago

Deployment of signature-based antivirus software requires installation of an engine that typically has kernel-level access to an endpoint's system resources. Signature-based antivirus software scans an endpoint's hard drive and memory, based on a predefined schedule and in real time when a file is accessed. If a known malware signature is detected, the software performs a predefined action, such as: ● Quarantine: Isolates the infected file so that it cannot infect the endpoint or other files ● Delete: Removes the infected file ● Alert: Notifies the user (and/or system administrator) that malware has been detected

upvoted 7 times

csco10320953 Most Recent 2 years, 1 month ago

I go with CDE- Since its signature based ,There is no need /important of notification to admin .

upvoted 1 times

cjoyce1980 2 years, 2 months ago

This is a question on Palo Alto Beacon platform and it states that the correct answers are Quarantine, Delete & Alert

upvoted 4 times

Bubu3k 3 years ago

page 123 of the study guide: If a known malware signature is detected, the software performs a predefined action, such as: ● Quarantine: Isolates the infected file so that it cannot infect the endpoint or other files ● Delete: Removes the infected file ● Alert: Notifies the user (and/or system administrator) that malware has been detected

upvoted 5 times

Question #49 *Topic 1*

Which option is a Prisma Access security service?

A. Compute Security

B. Firewall as a Service (FWaaS)

C. Virtual Private Networks (VPNs)

D. Software-defined wide-area networks (SD-WANs)

Suggested Answer: *B*

Official Answer: B

Community vote distribution

B (100%)

blahblah1234567890000 Most Recent 1 year, 11 months ago

Prisma Access provides firewall as a service (FWaaS) that protects branch offices from threats while also providing the security services expected from a next-generation firewall. The full spectrum of FWaaS includes threat prevention, URL filtering, sandboxing, and more.

upvoted 1 times

Question #50 *Topic 1*

Which pillar of Prisma Cloud application security addresses ensuring that your cloud resources and SaaS applications are correctly configured?

A. visibility, governance, and compliance

B. network protection

C. dynamic computing

D. compute security

Suggested Answer: *A*

Official Answer: A

Community vote distribution

A (100%)

blahblah1234567890000 Most Recent 1 year, 11 months ago

Forgot to choose my answer, its A. See my other replies with quotes from the study guide.

upvoted 3 times

blahblah1234567890000 1 year, 11 months ago

Compute security The cloud native landscape is constantly evolving with new technologies and levels of abstraction. Hosts, containers, and serverless workloads provide unique benefits and have different security requirements. Prisma Cloud provides best-in-class solutions for securing any type of cloud native workload throughout the development lifecycle.Cloud governance and compliance Ensuring that your cloud resources and SaaS applications are correctly configured and adhere to your organization's security standards from day one is essential to prevent successful attacks. Also, making sure that these applications, and the data they collect and store, are properly protected and compliant is critical to avoid costly fines, a tarnished image, and loss of customer trust. Meeting security standards and maintaining compliant environments at scale, and across SaaS applications, is the new expectation for security teams.Network protection Network protection must be adapted for cloud native environments while still enforcing consistent policies across hybrid environments. Prisma Cloud detects and prevents network anomalies by enforcing container-level micro-segmentation, inspecting traffic flow logs, and leveraging advanced Layer 7 threat protection.Dynamic computing fabric: Conventional, static computing environments are transformed into dynamic fabrics (private or hybrid clouds) where underlying resources such as network devices, storage, and servers can be fluidly engaged in whatever combination best meets the needs of the organization at any given point in time.

upvoted 2 times

blahblah1234567890000 1 year, 11 months ago

Compute security The cloud native landscape is constantly evolving with new technologies and levels of abstraction. Hosts, containers, and serverless workloads provide unique benefits and have different security requirements. Prisma Cloud provides best-in-class solutions for securing any type of cloud native workload throughout the development lifecycle.

upvoted 2 times

blahblah1234567890000 1 year, 11 months ago

Cloud governance and compliance Ensuring that your cloud resources and SaaS applications are correctly configured and adhere to your organization's security standards from day one is essential to prevent successful attacks. Also, making sure that these applications, and the data they collect and store, are properly protected and compliant is critical to avoid costly fines, a tarnished image, and loss of customer trust. Meeting security standards and maintaining compliant environments at scale, and across SaaS applications, is the new expectation for security teams.

upvoted 1 times

blahblah1234567890000 1 year, 11 months ago

Cloud governance and compliance Ensuring that your cloud resources and SaaS applications are correctly configured and adhere to your organization's security standards from day one is essential to prevent successful attacks. Also, making sure that these applications, and the data they collect and store, are properly protected and compliant is critical to avoid costly fines, a tarnished image, and loss of customer trust. Meeting security standards and maintaining compliant environments at scale, and across SaaS applications, is the new expectation for security teams.Network protection Network protection must be adapted for cloud native environments while still enforcing consistent policies across hybrid environments. Prisma Cloud detects and prevents network anomalies by enforcing container-level micro-segmentation, inspecting traffic flow logs, and leveraging advanced Layer 7 threat protection.Dynamic computing fabric: Conventional, static computing environments are transformed into dynamic fabrics (private or hybrid clouds) where underlying resources such as network devices, storage, and servers can be fluidly engaged in whatever combination best meets the needs of the organization at any given point in time.

upvoted 1 times

blahblah1234567890000 1 year, 11 months ago

Network protection Network protection must be adapted for cloud native environments while still enforcing consistent policies across hybrid environments. Prisma Cloud detects and prevents network anomalies by enforcing container-level micro-segmentation, inspecting traffic flow logs, and leveraging advanced Layer 7 threat protection.

upvoted 1 times

blahblah1234567890000 1 year, 11 months ago

Network protection Network protection must be adapted for cloud native environments while still enforcing consistent policies across hybrid environments. Prisma Cloud detects and prevents network anomalies by enforcing container-level micro-segmentation, inspecting traffic flow logs, and leveraging advanced Layer 7 threat protection.Dynamic computing fabric: Conventional, static computing environments are transformed into dynamic fabrics (private or hybrid clouds) where underlying resources such as network devices, storage, and servers can be fluidly engaged in whatever combination best meets the needs of the organization at any given point in time.

upvoted 1 times

blahblah1234567890000 1 year, 11 months ago

Dynamic computing fabric: Conventional, static computing environments are transformed into dynamic fabrics (private or hybrid clouds) where underlying resources such as network devices, storage, and servers can be fluidly engaged in whatever combination best meets the needs of the organization at any given point in time.

upvoted 1 times

Question #51 *Topic 1*

Which item accurately describes a security weakness that is caused by implementing a `ports first` data security solution in a traditional data center?

A. You may have to use port numbers greater than 1024 for your business-critical applications.

B. You may have to open up multiple ports and these ports could also be used to gain unauthorized entry into your datacenter.

C. You may not be able to assign the correct port to your business-critical applications.

D. You may not be able to open up enough ports for your business-critical applications which will increase the attack surface area.

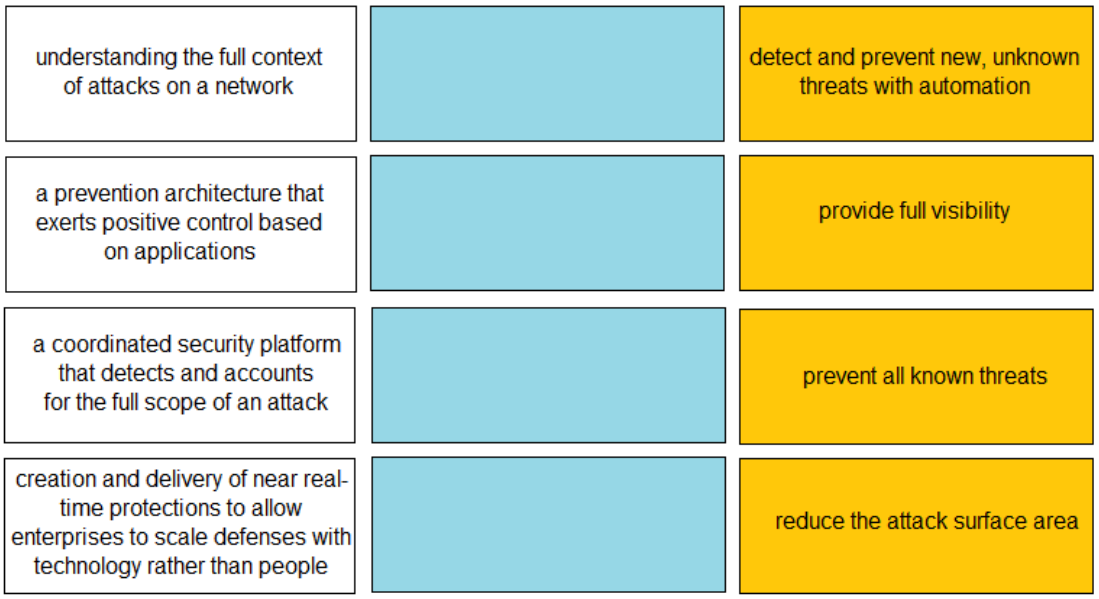
Suggested Answer: *B*
Official Answer: B

Currently there are no comments in this discussion, be the first to comment!

DRAG DROP -

Match each description to a Security Operating Platform key capability.

Select and Place:



Suggested Answer:



understanding the full context of attacks on a network
creation and delivery of near real-time protections to allow enterprises to scale defenses with technology rather than people
detect and prevent new, unknown threats with automation
a prevention architecture that exerts positive control based on applications
understanding the full context of attacks on a network
provide full visibility
a coordinated security platform that detects and accounts for the full scope of an attack
a coordinated security platform that detects and accounts for the full scope of an attack
prevent all known threats
creation and delivery of near real-time protections to allow enterprises to scale defenses with technology rather than people
a prevention architecture that exerts positive control based on applications
reduce the attack surface area

Syfusion Most Recent 2 years, 1 month ago

Answer appear to be correct Study Guide page 65 for reference

upvoted 1 times

blahblah1234567890000 2 years, 11 months ago

● Provide full visibility: For network administrators and security practitioners to understand the full context of an attack, visibility of all users and devices is provided across the organization's network, endpoint, cloud, and SaaS applications.

upvoted 2 times

blahblah1234567890000 2 years, 11 months ago

● Provide full visibility: For network administrators and security practitioners to understand the full context of an attack, visibility of all users and devices is provided across the organization's network, endpoint, cloud, and SaaS applications.● Reduce the attack surface: Best-of-breed technologies that are natively integrated provide a prevention architecture that inherently reduces the attack surface. This type of architecture allows organizations to exert positive control based on applications, users, and content, with support for open communication, orchestration, and visibility. ● Prevent all known threats, fast: A coordinated security platform accounts for the full scope of an attack across the various security controls that compose the security posture, thus enabling organizations to quickly identify and block known threats. ● Detect and prevent new, unknown threats with automation: Security that simply detects threats and requires a manual response is too little, too late. Automated creation and delivery of near-real-time protections against new threats to the various security solutions in the organization's environments enable dynamic policy updates. These updates are designed to allow enterprises to scale defenses with technology, rather than people.

upvoted 2 times

blahblah1234567890000 2 years, 11 months ago

● Reduce the attack surface: Best-of-breed technologies that are natively integrated provide a prevention architecture that inherently reduces the attack surface. This type of architecture allows organizations to exert positive control based on applications, users, and content, with support for open communication, orchestration, and visibility. ● Prevent all known threats, fast: A coordinated security platform accounts for the full scope of an attack across the various security controls that compose the security posture, thus enabling organizations to quickly identify and block known threats. ● Detect and prevent new, unknown threats with automation: Security that simply detects threats and requires a manual response is too little, too late. Automated creation and delivery of near-real-time protections against new threats to the various security solutions in the organization's environments enable dynamic policy updates. These updates are designed to allow enterprises to scale defenses with technology, rather than people.

upvoted 2 times

Question #53 *Topic 1*

Which statement describes DevOps?

A. DevOps is its own separate team

B. DevOps is a set of tools that assists the Development and Operations teams throughout the software delivery process

C. DevOps is a combination of the Development and Operations teams

D. DevOps is a culture that unites the Development and Operations teams throughout the software delivery process

Suggested Answer: *D*
Official Answer: D

Community vote distribution
D (100%)

Jhonc Highly Voted 3 years, 7 months ago
D is correct
upvoted 5 times

Merlin0o Highly Voted 2 years, 6 months ago
D is correct
upvoted 5 times

rob899 Most Recent 1 year, 11 months ago
Answer is D. Straight from the Study guide page 168 "DevOps solves these problems by uniting Development and Operations teams throughout the entire software delivery process, enabling them to discover and remediate issues earlier, automate testing and deployment, and reduce time to market."
upvoted 1 times

tjanki 2 years, 7 months ago
DevOps is not: ● A combination of the Dev and Ops teams: There still are two teams; they just operate in a communicative, collaborative way. ● Its own separate team: There is no such thing as a “DevOps engineer.” Although some companies may appoint a “DevOps team” as a pilot when trying to transition to a DevOps culture, DevOps refers to a culture where developers, testers, and operations personnel cooperate throughout the entire software delivery lifecycle. ● A tool or set of tools: Although there are tools that work well with a DevOps model or help promote DevOps culture, DevOps ultimately is a strategy, not a tool. ● Automation: Although automation is very important for a DevOps culture, it alone does not define DevOps.
upvoted 2 times

error_909 2 years, 11 months ago
"DevOps solves these problems by uniting Development and Operations teams throughout the entire software delivery process, enabling them to discover and remediate issues earlier, automate testing and deployment, and reduce time to market"
upvoted 2 times

Question #54 *Topic 1*

Which product from Palo Alto Networks enables organizations to prevent successful cyberattacks as well as simplify and strengthen security processes?

A. Expedition

B. AutoFocus

C. MineMeld

D. Cortex XDR

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

blahblah1234567890000 Most Recent 1 year, 11 months ago

From a business perspective, XDR platforms enable organizations to prevent successful cyberattacks as well as simplify and strengthen security processes.

upvoted 1 times

Question #55 *Topic 1*

Which network firewall operates up to Layer 4 (Transport layer) of the OSI model and maintains information about the communication sessions which have been established between hosts on trusted and untrusted networks?

A. Group policy

B. Stateless

C. Stateful

D. Static packet-filter

Suggested Answer: *C*

Official Answer: C

Community vote distribution

C (100%)

blahblah1234567890000 Most Recent 1 year, 11 months ago

Stateful packet inspection firewalls Second-generation stateful packet inspection (also known as dynamic packet filtering) firewalls have the following characteristics: ● They operate up to Layer 4 (Transport layer) of the OSI model and maintain state information about the communication sessions that have been established between hosts on the trusted and untrusted networks. ● They inspect individual packet headers to determine source and destination IP address, protocol (TCP, UDP, and ICMP), and port number (during session establishment only) to determine whether the session should be allowed, blocked, or dropped based on configured firewall rules. ● After a permitted connection is established between two hosts, the firewall creates and deletes firewall rules for individual connections as needed, thus effectively creating a tunnel that allows traffic to flow between the two hosts without further inspection of individual packets during the session. ● This type of firewall is very fast, but it is port-based and it is highly dependent on the trustworthiness of the two hosts because individual packets aren't inspected after the connection is established.

upvoted 1 times

Question #56 *Topic 1*

Which subnet does the host 192.168.19.36/27 belong?

A. 192.168.19.0

B. 192.168.19.16

C. 192.168.19.64

D. 192.168.19.32

Suggested Answer: *D*
Official Answer: D

dax Most Recent 2 years, 1 month ago

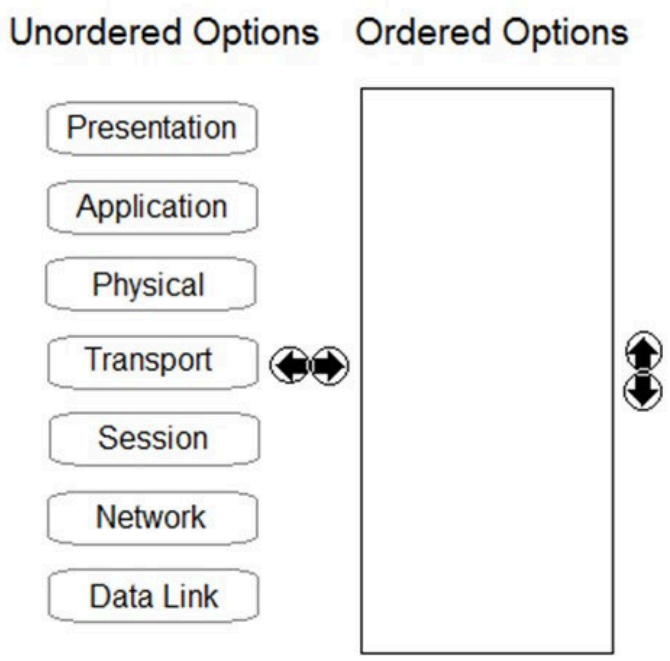
D /27 is 32 subnets

upvoted 1 times

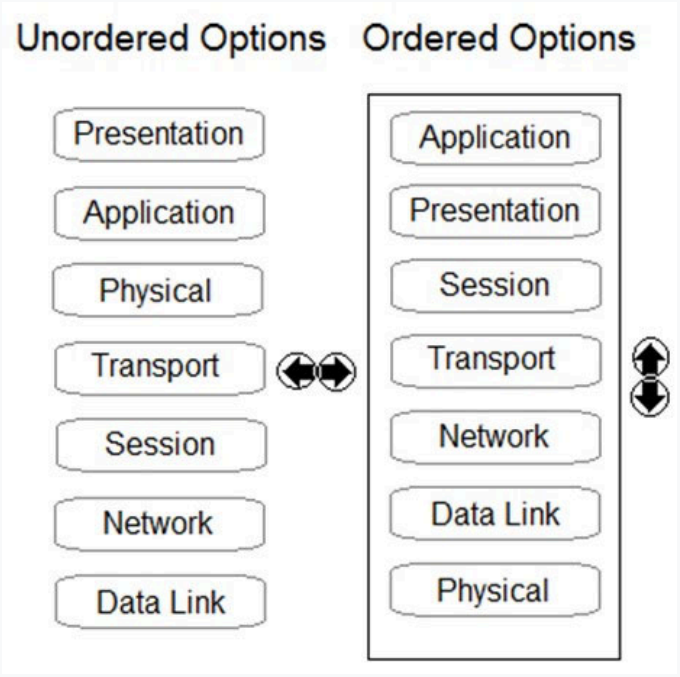
DRAG DROP -

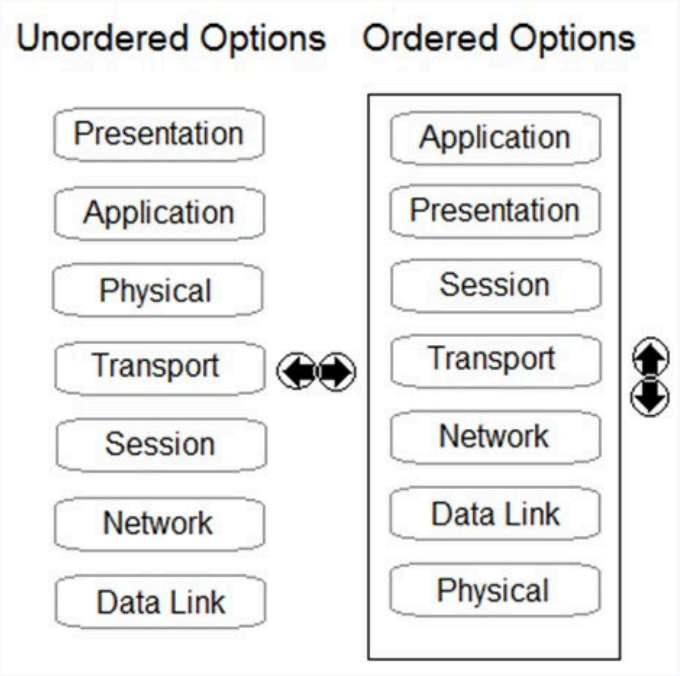
Order the OSI model with Layer7 at the top and Layer1 at the bottom.

Select and Place:



Suggested Answer:





nillie Most Recent 2 years ago

All People Seem To Need Data Processing

upvoted 1 times

Question #58 *Topic 1*

How does adopting a serverless model impact application development?

A. costs more to develop application code because it uses more compute resources

B. slows down the deployment of application code, but it improves the quality of code development

C. reduces the operational overhead necessary to deploy application code

D. prevents developers from focusing on just the application code because you need to provision the underlying infrastructure to run the code

Suggested Answer: *C*

Official Answer: C

Community vote distribution

C (100%)

blahblah1234567890000 Most Recent 1 year, 11 months ago

List three advantages of serverless computing over CaaS: - Reduce costs - Increase agility - Reduce operational overhead

upvoted 3 times

Question #59 *Topic 1*

In addition to integrating the network and endpoint components, what other component does Cortex integrate to speed up IoC investigations?

A. Computer

B. Switch

C. Infrastructure

D. Cloud

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

blahblah1234567890000 Most Recent 1 year, 11 months ago

I agree, it should be cloud.

upvoted 2 times

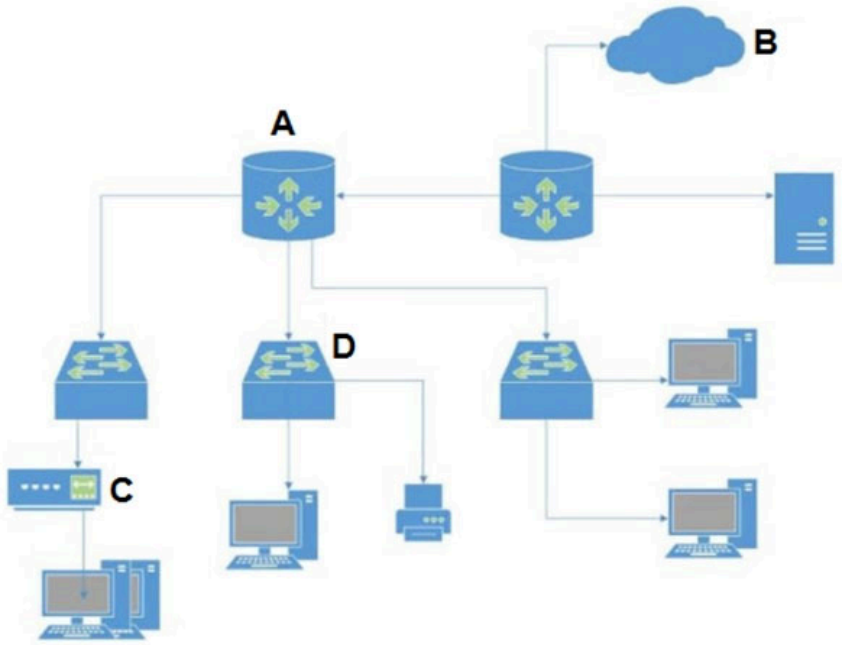
Merlin0o 2 years ago

Should be D: Page 161 of the guide: "Cortex XDR detection and response uses network, cloud, and endpoints as sensors"

upvoted 3 times

Question #60 *Topic 1*

In the attached network diagram, which device is the switch?



A. A

B. B

C. C

D. D

Suggested Answer: *D*
Official Answer: D

duckduckgooo Most Recent 1 year, 10 months ago
Picture is a switch icon. D is correct. A is a router
upvoted 1 times

A__2__111 2 years, 2 months ago
The actual question asks which is a router
upvoted 1 times

Question #61 *Topic 1*

In SecOps, what are two of the components included in the identify stage? (Choose two.)

A. Initial Research

B. Change Control

C. Content Engineering

D. Breach Response

Suggested Answer: *A, C*

Official Answer: AC

Community vote distribution

AC (100%)

blahblah1234567890000 Most Recent 1 year, 11 months ago

Pg. 206 of guide

upvoted 2 times

Question #62 *Topic 1*

Data Loss Prevention (DLP) and Cloud Access Security Broker (CASB) fall under which Prisma access service layer?

A. Network

B. Management

C. Cloud

D. Security

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

blahblah1234567890000 Most Recent 1 year, 11 months ago

A SASE solution converges networking and security services into one unified, cloud-delivered solution (see Figure 3-12) that includes the following: ● Networking ○ Software-defined wide-area networks (SD-WANs) ○ Virtual private networks (VPNs) ○ Zero Trust network access (ZTNA) ○ Quality of Service (QoS) ● Security ○ Firewall as a service (FWaaS) ○ Domain Name System (DNS) security ○ Threat prevention ○ Secure web gateway (SWG) ○ Data loss prevention (DLP) ○ Cloud access security broker (CASB)

upvoted 4 times

Question #63 *Topic 1*

In which two cloud computing service models are the vendors responsible for vulnerability and patch management of the underlying operating system? (Choose two.)

A. SaaS

B. PaaS

C. On-premises

D. IaaS

Suggested Answer: *A, B*
Official Answer: AB

cert111 2 years ago
Why isn't C included?On-Prem is your own HW and responsibility.
upvoted 1 times

cert111 2 years ago
Why isn't C included?
upvoted 1 times

Merlin0o Most Recent 1 year, 12 months ago
On-Prem is your own HW and responsibility.
upvoted 4 times

Question #64 *Topic 1*

SecOps consists of interfaces, visibility, technology, and which other three elements? (Choose three.)

A. People

B. Accessibility

C. Processes

D. Understanding

E. Business

Suggested Answer: *A, C, E*

Official Answer: ACE

Community vote distribution

ACE (100%)

blahblah1234567890000 Highly Voted 1 year, 11 months ago

The six pillars include: 1. Business (goals and outcomes) 2. People (who will perform the work) 3. Interfaces (external functions to help achieve goals) 4. Visibility (information needed to accomplish goals) 5. Technology (capabilities needed to provide visibility and enable people) 6. Processes (tactical steps required to execute on goals) All elements must tie back to the business itself and the goals of the security operations

upvoted 6 times

Merlin0o 2 years ago

SecOps consists of six elements: 1. Business (goals and outcomes) 2. People (who will perform the work) 3. Interfaces (external functions to help achieve goals) 4. Visibility (information needed to accomplish goals) 5. Technology (capabilities needed to provide visibility and enable people) 6. Processes (tactical steps needed to execute on goals)

upvoted 4 times

Question #65 *Topic 1*

Which IoT connectivity technology is provided by satellites?

A. 4G/LTE

B. VLF

C. L-band

D. 2G/2.5G

Suggested Answer: *C*

Official Answer: C

Community vote distribution

C (100%)

blahblah1234567890000 1 year, 11 months ago

2G/2.5G: 2G connectivity remains a prevalent and viable IoT connectivity option due to the low cost of 2G modules, relatively long battery life, and large installed base of 2G sensors and M2M applications. ○ 3G: IoT devices with 3G modules use either Wideband Code Division Multiple Access (W-CDMA) or Evolved High Speed Packet Access (HSPA+ and Advanced HSPA+) to achieve data transfer rates of 384Kbps to 168Mbps. ○ 4G/Long-Term Evolution (LTE): 4G/LTE networks enable real-time IoT use cases, such as autonomous vehicles, with 4G LTE Advanced Pro delivering speeds in excess of 3Gbps and less than 2 milliseconds of latency. ○ 5G: 5G cellular technology provides significant enhancements compared to 4G/LTE networks and is backed by ultra-low latency, massive connectivity and scalability for IoT devices, more efficient use of the licensed spectrum, and network slicing for application traffic prioritization.Satellite: ○ C-band: C-band satellite operates in the 4 to 8 gigahertz (GHz) range. It is used in some Wi-Fi devices and cordless phones, and in surveillance and weather radar systems. ○ L-band: L-band satellite operates in the 1 to 2GHz range. It commonly is used for radar, global positioning systems (GPSs), radio, and telecommunications applications.

upvoted 2 times

blahblah1234567890000 1 year, 11 months ago

Selected Answer: C

2G/2.5G: 2G connectivity remains a prevalent and viable IoT connectivity option due to the low cost of 2G modules, relatively long battery life, and large installed base of 2G sensors and M2M applications. ○ 3G: IoT devices with 3G modules use either Wideband Code Division Multiple Access (W-CDMA) or Evolved High Speed Packet Access (HSPA+ and Advanced HSPA+) to achieve data transfer rates of 384Kbps to 168Mbps. ○ 4G/Long-Term Evolution (LTE): 4G/LTE networks enable real-time IoT use cases, such as autonomous vehicles, with 4G LTE Advanced Pro delivering speeds in excess of 3Gbps and less than 2 milliseconds of latency. ○ 5G: 5G cellular technology provides significant enhancements compared to 4G/LTE networks and is backed by ultra-low latency, massive connectivity and scalability for IoT devices, more efficient use of the licensed spectrum, and network slicing for application traffic prioritization.

upvoted 2 times

blahblah1234567890000 Most Recent 1 year, 11 months ago

Satellite: ○ C-band: C-band satellite operates in the 4 to 8 gigahertz (GHz) range. It is used in some Wi-Fi devices and cordless phones, and in surveillance and weather radar systems. ○ L-band: L-band satellite operates in the 1 to 2GHz range. It commonly is used for radar, global positioning systems (GPSs), radio, and telecommunications applications.

upvoted 1 times

Question #66 *Topic 1*

What does Palo Alto Networks Cortex XDR do first when an endpoint is asked to run an executable?

A. run a static analysis

B. check its execution policy

C. send the executable to WildFire

D. run a dynamic analysis

Suggested Answer: *B*
Official Answer: B

Alinutzu Most Recent 1 year, 9 months ago

B. Phase 1: Evaluation of Child Process Protection Policy When a user attempts to run an executable, the operating system attempts to run the executable as a process. If the process tries to launch any child processes, the Cortex XDR agent first evaluates the child process protection policy.
upvoted 1 times

Question #67 *Topic 1*

What is the key to `taking down` a botnet?

A. prevent bots from communicating with the C2

B. install openvas software on endpoints

C. use LDAP as a directory service

D. block Docker engine software on endpoints

Suggested Answer: *A*

Official Answer: A

Community vote distribution

A (100%)

blahblah1234567890000 Most Recent 1 year, 11 months ago

Answer is a. This is how botnets are typically taken down.

upvoted 3 times

Question #68 *Topic 1*

How does Prisma SaaS provide protection for Sanctioned SaaS applications?

A. Prisma SaaS connects to an organizations internal print and file sharing services to provide protection and sharing visibility

B. Prisma SaaS does not provide protection for Sanctioned SaaS applications because they are secure

C. Prisma access uses Uniform Resource Locator (URL) Web categorization to provide protection and sharing visibility

D. Prisma SaaS connects directly to sanctioned external service providers SaaS application service to provide protection and sharing visibility

Suggested Answer: *D*

Official Answer: D

Community vote distribution



Alinutzu Most Recent 1 year, 9 months ago

D. Prisma SaaS delivers complete visibility and granular enforcement across all user, folder and file activity within sanctioned SaaS applications, providing detailed analysis and analytics on usage without requiring any additional hardware, software or network changes.

upvoted 1 times

blahblah1234567890000 2 years, 11 months ago

Prisma SaaS connects directly to the applications themselves, therefore providing continuous silent monitoring of the risks within the sanctioned SaaS applications, with detailed visibility that is not possible with traditional security solutions.

upvoted 2 times

Question #69 *Topic 1*

Which type of Software as a Service (SaaS) application provides business benefits, is fast to deploy, requires minimal cost and is infinitely scalable?

A. Benign

B. Tolerated

C. Sanctioned

D. Secure

Suggested Answer: *C*
Official Answer: C

duckduckgooo Most Recent 1 year, 10 months ago

ANswer is C https://www.cloudcodes.com/blog/enterprise-data-security-sanctioned-unsanctioned-apps.html

upvoted 1 times

Question #70 *Topic 1*

How does DevSecOps improve the Continuous Integration/Continuous Deployment (CI/CD) pipeline?

A. DevSecOps improves pipeline security by assigning the security team as the lead team for continuous deployment

B. DevSecOps ensures the pipeline has horizontal intersections for application code deployment

C. DevSecOps unites the Security team with the Development and Operations teams to integrate security into the CI/CD pipeline

D. DevSecOps does security checking after the application code has been processed through the CI/CD pipeline

Suggested Answer: *C*

Official Answer: C

Community vote distribution

C (100%)

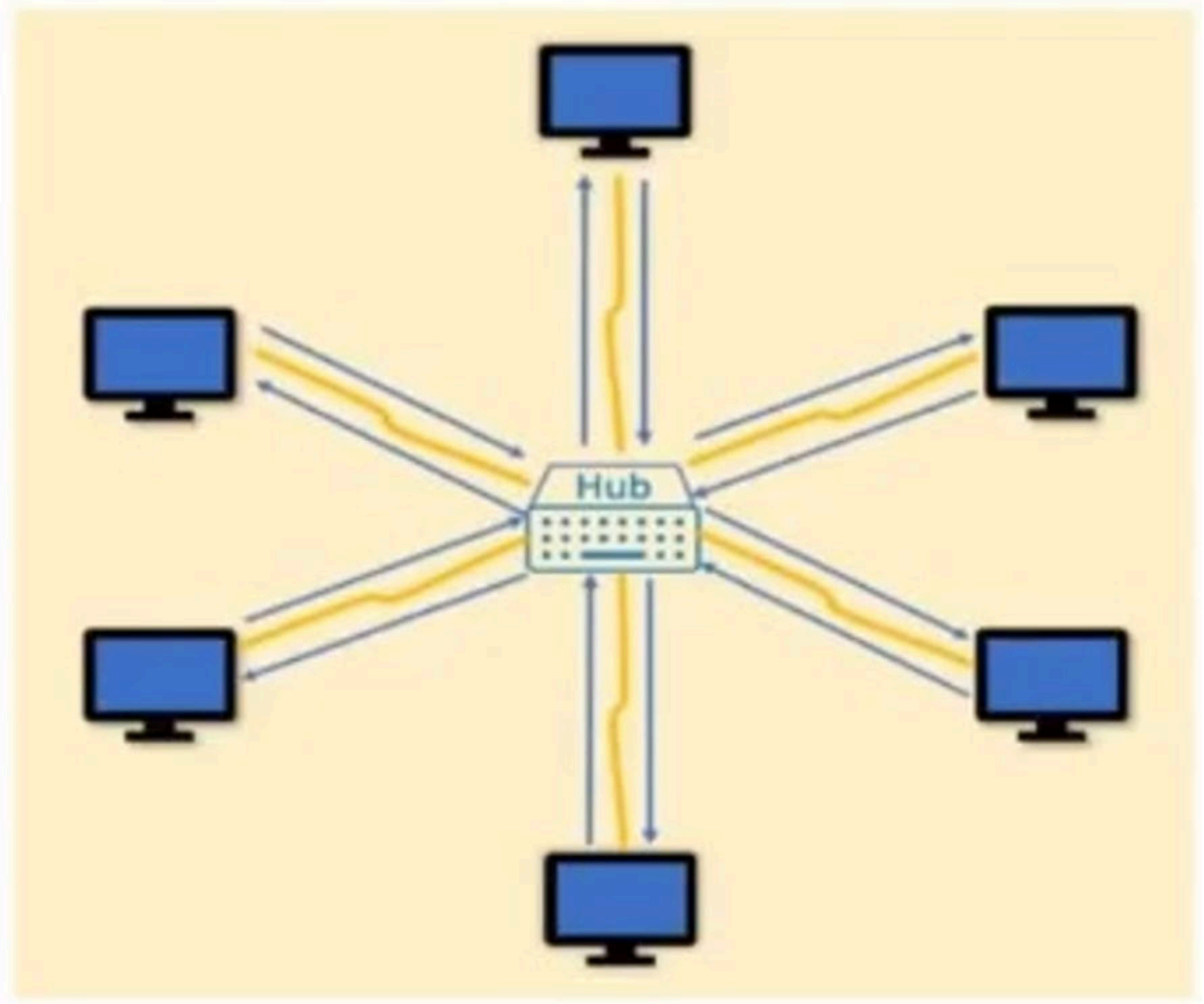
blahblah1234567890000 Most Recent 1 year, 11 months ago

DevSecOps takes the concept behind DevOps that developers and IT teams should work together closely, instead of separately, throughout software delivery and extends it to include security and integrate automated checks into the full CI/CD pipeline. The integration of the CI/CD pipeline takes care of the problem of security seeming like an outside force and instead allows developers to maintain their usual speed without compromising data security

upvoted 1 times

Question #71 *Topic 1*

Which type of LAN technology is being displayed in the diagram?



A. Star Topology

B. Spine Leaf Topology

C. Mesh Topology

D. Bus Topology

Suggested Answer: *A*

Official Answer: A

Community vote distribution

A (100%)

blahblah1234567890000 Highly Voted 3 years, 11 months ago

Selected Answer: A

Star topology, just google it to confirm.

upvoted 6 times

blahblah1234567890000 Highly Voted 3 years, 11 months ago

Star topology, just google it to confirm.I was like wait, I got that wrong! A is correct

upvoted 6 times

duckduckgooo 3 years, 10 months ago

I was like wait, I got that wrong! A is correct

upvoted 3 times

kirmanis Most Recent 1 year, 11 months ago

Star Topology. Mesh will have each device connected to every other device. Secondly, for easier remembrance, it does look like a star. Mesh looks like a mess.

upvoted 1 times

Javdash 3 years, 3 months ago

Because

upvoted 3 times

AnBo 3 years, 5 months ago

https://www.dnsstuff.com/what-is-network-topology#star-topology

upvoted 1 times

AnBo 3 years, 7 months ago

I agree. The diagram is a star topology. The web administrator will need to correct this.

upvoted 2 times

cert111 3 years, 11 months ago

Should be A. This is a star topology, not a mesh.

upvoted 4 times

Question #72 *Topic 1*

An Administrator wants to maximize the use of a network address. The network is 192.168.6.0/24 and there are three subnets that need to be created that can not overlap. Which subnet would you use for the network with 120 hosts?
Requirements for the three subnets:
Subnet 1: 3 host addresses -
Subnet 2: 25 host addresses -
Subnet 3: 120 host addresses -

A. 192.168.6.168/30

B. 192.168.6.0/25

C. 192.168.6.160/29

D. 192.168.6.128/27

Suggested Answer: *B*
Official Answer: B

Currently there are no comments in this discussion, be the first to comment!

Question #73 *Topic 1*

Which two network resources does a directory service database contain? (Choose two.)

A. Services

B. /etc/shadow files

C. Users

D. Terminal shell types on endpoints

Suggested Answer: *A, C*

Official Answer: AC

Community vote distribution

AC (100%)

blahblah1234567890000 Most Recent 1 year, 11 months ago

A directory service is a database that contains information about users, resources, and services in a network.

upvoted 2 times

Question #74 *Topic 1*

Which model would a customer choose if they want full control over the operating system(s) running on their cloud computing platform?

A. SaaS

B. DaaS

C. PaaS

D. IaaS

Suggested Answer: *D*
Official Answer: D

duckduckgooo Most Recent 1 year, 10 months ago
Infrastructure as a Service , D, is correct
upvoted 2 times

Question #75 *Topic 1*

What is a key advantage and key risk in using a public cloud environment?

A. Multi-tenancy

B. Dedicated Networks

C. Dedicated Hosts

D. Multiplexing

Suggested Answer: *A*

Official Answer: A

Community vote distribution

A (100%)

blahblah1234567890000 Most Recent 1 year, 11 months ago

Multitenancy is a key characteristic of the public cloud, and an important risk. Although public cloud providers strive to ensure isolation between their various customers, the infrastructure and resources in the public cloud are shared. Inherent risks in a shared environment include misconfigurations, inadequate or ineffective processes and controls, and the “noisy neighbor” problem (excessive network traffic, disk I/O, or processor use can negatively impact other customers sharing the same resource). In hybrid and multicloud environments that connect numerous public and/or private clouds, the delineation becomes blurred, complexity increases, and security risks become more challenging to address.

upvoted 3 times

Merlin0o 2 years ago

Page 190 of the study guide: "Multitenancy is a key characteristic of the public cloud, and an important risk"

upvoted 2 times

Question #76 *Topic 1*

Which three layers of the OSI model correspond to the Application Layer (L4) of the TCP/IP model?

A. Session, Transport, Network

B. Application, Presentation, and Session

C. Physical, Data Link, Network

D. Data Link, Session, Transport

Suggested Answer: *B*
Official Answer: B

Community vote distribution
B (100%)

blahblah1234567890000 1 year, 11 months ago

Selected Answer: B

Application (Layer 4 or L4): This layer loosely corresponds to Layers 5 through 7 of the OSI model. Transport (Layer 3 or L3): This layer corresponds to Layer 4 of the OSI model. Internet (Layer 2 or L2): This layer corresponds to Layer 3 of the OSI model. Network Access (Layer 1 or L1): This layer corresponds to Layers 1 and 2 of the OSI model

upvoted 2 times

blahblah1234567890000 1 year, 11 months ago

Application (Layer 4 or L4): This layer loosely corresponds to Layers 5 through 7 of the OSI model. Transport (Layer 3 or L3): This layer corresponds to Layer 4 of the OSI model. Internet (Layer 2 or L2): This layer corresponds to Layer 3 of the OSI model. Network Access (Layer 1 or L1): This layer corresponds to Layers 1 and 2 of the OSI modelThe 7 layers of the OSI model. The layers are: Layer 1—Physical; Layer 2—Data Link; Layer 3—Network; Layer 4—Transport; Layer 5—Session; Layer 6—Presentation; Layer 7—Application.

upvoted 2 times

blahblah1234567890000 Most Recent 1 year, 11 months ago

The 7 layers of the OSI model. The layers are: Layer 1—Physical; Layer 2—Data Link; Layer 3—Network; Layer 4—Transport; Layer 5—Session; Layer 6—Presentation; Layer 7—Application.

upvoted 1 times

Question #77 *Topic 1*

Which NGFW feature is used to provide continuous identification, categorization, and control of known and previously unknown SaaS applications?

A. User-ID

B. Device-ID

C. App-ID

D. Content-ID

Suggested Answer: *C*

Official Answer: C

Community vote distribution

C (100%)

blahblah1234567890000 Most Recent 1 year, 11 months ago

App-ID™ technology leverages the power of the broad global community to provide continuous identification, categorization, and granular risk-based control of known and previously unknown SaaS applications, ensuring new applications are discovered automatically as they become popular.

upvoted 3 times

Question #78 *Topic 1*

What is a common characteristic of serverless and containers?

A. run for prolonged period of time

B. run on specific hosting platforms

C. automate and dynamically scale workloads

D. open source

Suggested Answer: *C*
Official Answer: C

Alinutzu Most Recent 1 year, 9 months ago

C. Similarities Between Serverless and Containers Both allow development teams to: Deploy app code consistently at all times. Save the cost and avoid the complexity of VMs. Automate & dynamically scale workloads.

upvoted 1 times

Question #79 *Topic 1*

Which method is used to exploit vulnerabilities, services, and applications?

A. encryption

B. port scanning

C. DNS tunneling

D. port evasion

Suggested Answer: *D*
Official Answer: D

Alinutzu Most Recent 1 year, 9 months ago

B. Port scanning Port scanning is a method used to exploit vulnerabilities, services, and applications. It involves scanning a target system or network to identify open ports, services, and potential vulnerabilities. Attackers use port scanning as a reconnaissance technique to discover entry points into a system that can be exploited. Once open ports and services are identified, attackers can attempt to exploit known vulnerabilities or weaknesses in the services or applications running on those ports. This makes port scanning an essential step in the process of identifying and potentially exploiting security weaknesses in a target system.

upvoted 2 times

blahblah1234567890000 2 years, 11 months ago

Attack communication traffic is usually hidden with various techniques and tools, including: ● Encryption with SSL, SSH (Secure Shell), or some other custom or proprietary encryption ● Circumvention via proxies, remote access tools, or tunneling. In some instances, use of cellular networks enables complete circumvention of the target network for attack C2 traffic. ● Port evasion using network anonymizers or port hopping to traverse over any available open ports ● Fast Flux (or Dynamic DNS) to proxy through multiple infected endpoints or multiple, ever-changing C2 servers to reroute traffic and make determination of the true destination or attack source difficult ● DNS tunneling is used for C2 communications and data infiltration (for examp

upvoted 1 times

blahblah1234567890000 2 years, 11 months ago

Attack communication traffic is usually hidden with various techniques and tools, including: ● Encryption with SSL, SSH (Secure Shell), or some other custom or proprietary encryption ● Circumvention via proxies, remote access tools, or tunneling. In some instances, use of cellular networks enables complete circumvention of the target network for attack C2 traffic. ● Port evasion using network anonymizers or port hopping to traverse over any available open ports ● Fast Flux (or Dynamic DNS) to proxy through multiple infected endpoints or multiple, ever-changing C2 servers to reroute traffic and make determination of the true destination or attack source difficult ● DNS tunneling is used for C2 communications and data infiltration (for exampPort scanning would be use to identify services prior to exploitation so it would be in tandem but none of these options are actually used for exploitation.

upvoted 1 times

blahblah1234567890000 2 years, 11 months ago

Port scanning would be use to identify services prior to exploitation so it would be in tandem but none of these options are actually used for exploitation.

upvoted 2 times

Question #80 *Topic 1*

Which security component should you configure to block viruses not seen and blocked by the perimeter firewall?

A. endpoint antivirus software

B. strong endpoint passwords

C. endpoint disk encryption

D. endpoint NIC ACLs

Suggested Answer: *A*
Official Answer: A

Community vote distribution
A (100%)

vassily Most Recent 2 years ago
Answer is A
upvoted 1 times

mkucuk89 2 years, 1 month ago
Answer is A
upvoted 1 times

leipeG 2 years, 3 months ago
To block viruses that are not seen and blocked by the perimeter firewall, you should configure: A. Endpoint antivirus software Endpoint antivirus software is designed to scan and detect viruses and malware on individual devices (endpoints) such as computers and mobile devices. It provides an additional layer of defense beyond the perimeter firewall by actively scanning files, processes, and network activity on the endpoint itself. This helps to identify and block threats that may bypass the perimeter firewall's initial inspection. Options B, C, and D are not specifically focused on antivirus protection and do not address the need to block viruses that might evade the perimeter firewall.
upvoted 1 times

cert111 3 years, 5 months ago
Encryption doesn't block viruses. Should be A.
upvoted 3 times

blahblah1234567890000 3 years, 5 months ago
It would be the endpoint AV
upvoted 4 times

Question #81 *Topic 1*

In which situation would a dynamic routing protocol be the quickest way to configure routes on a router?

A. the network is large

B. the network is small

C. the network has low bandwidth requirements

D. the network needs backup routes

Suggested Answer: *A*
Official Answer: A

Community vote distribution
A (100%)

splashy 2 years, 1 month ago

Selected Answer: A

Definitely A. D you would better achieve by creating static floating routes (with a lower AD) this is more CCNA knowledge but i think the same rules apply here.

upvoted 1 times

splashy 2 years, 1 month ago

Definitely A. D you would better achieve by creating static floating routes (with a lower AD) this is more CCNA knowledge but i think the same rules apply here.Then again ... in a very large OSPF network consisting of multiple autonomous systems, you could "publish" a default route to all devices within 1 autonomous system by 'default-information originate' (again Cisco perspective here). I still think A is the primary answer but D could be a secondary...

upvoted 1 times

splashy Most Recent 2 years, 1 month ago

Then again ... in a very large OSPF network consisting of multiple autonomous systems, you could "publish" a default route to all devices within 1 autonomous system by 'default-information originate' (again Cisco perspective here). I still think A is the primary answer but D could be a secondary...

upvoted 1 times

Syfusion 2 years, 2 months ago

Answer should be A Study Guide page 73 talks about differentiating between the two "Static routing is practical only in very small networks or for very limited, special-case routing scenarios (for example, a destination that's used as a backup route or is reachable only via a single router). However, static routing has low bandwidth requirements..." Therefore the remaining answer A is correct for Dynamic Routing

upvoted 1 times

Mutty 2 years, 2 months ago

The only possible answer is A. In most cases you will only be placing floating static routes as a backup.

upvoted 1 times

dax 2 years, 7 months ago

A. Dynamic routing is considered easy to configure on large networks, and also, it is more intuitive than static routing at a selection of the best route, detection of the route changes, and also a discovery of the remote networks.

upvoted 1 times

blahblah1234567890000 2 years, 11 months ago

Selected Answer: A

A static routing protocol requires that routes be created and updated manually on a router or other network device. If a static route is down, traffic can't be automatically rerouted unless an alternate route has been configured. Also, if the route is congested, traffic can't be automatically rerouted over the less congested alternate route. Static routing is practical only in very small networks or for very limited, special-case routing scenarios (for example, a destination that's used as a backup route or is reachable only via a single router). However, static routing has low bandwidth requirements (routing information isn't broadcast across the network) and some built-in security (users can route only to destinations that are specified in statically defined routes).

upvoted 2 times

blahblah1234567890000 2 years, 11 months ago

A static routing protocol requires that routes be created and updated manually on a router or other network device. If a static route is down, traffic can't be automatically rerouted unless an alternate route has been configured. Also, if the route is congested, traffic can't be automatically rerouted over the less congested alternate route. Static routing is practical only in very small networks or for very limited, special-case routing scenarios (for example, a destination that's used as a backup route or is reachable only via a single router). However, static routing has low bandwidth requirements (routing information isn't broadcast across the network) and some built-in security (users can route only to destinations that are specified in statically defined routes).The answer could be both a and d since both apply here but its asking specifically about which is quicker so I choose A.

upvoted 2 times

blahblah1234567890000 2 years, 11 months ago

The answer could be both a and d since both apply here but its asking specifically about which is quicker so I choose A.

upvoted 1 times

Question #82 *Topic 1*

Which of the following is an AWS serverless service?

A. Beta

B. Kappa

C. Delta

D. Lambda

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

blahblah1234567890000 Most Recent 1 year, 11 months ago

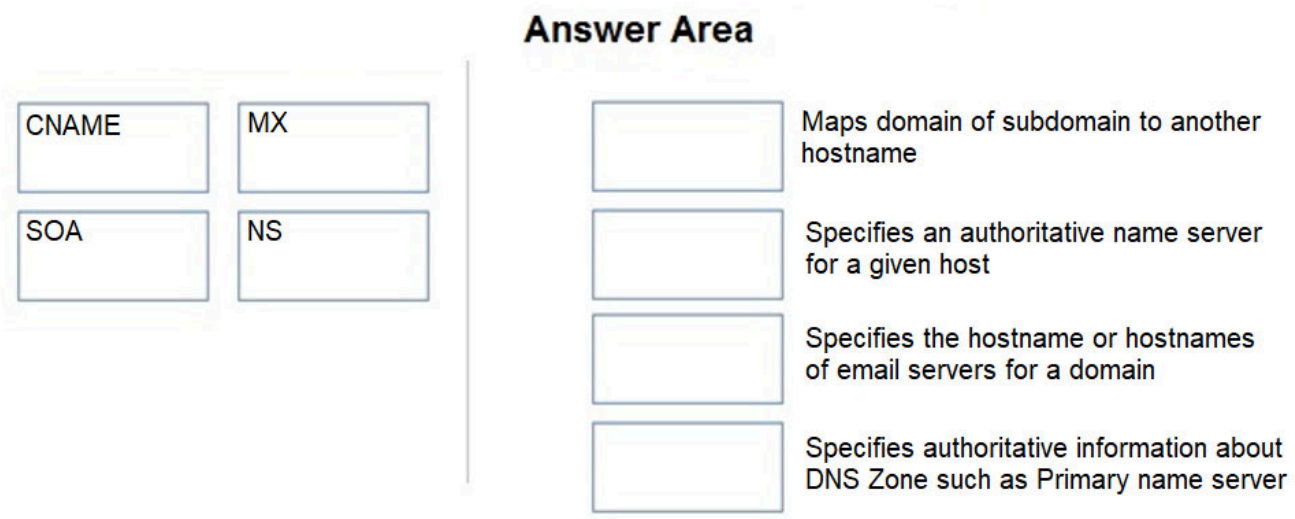
Examples of serverless environments include Amazon Lambda and Azure Functions. Many PaaS offerings, such as Pivotal Cloud Foundry, also are effectively serverless even if they have not historically been marketed as such. Although serverless may appear to lack the container-specific, cloud native attribute, containers are extensively used in the underlying implementations, even if those implementations are not exposed to end users directly.

upvoted 2 times

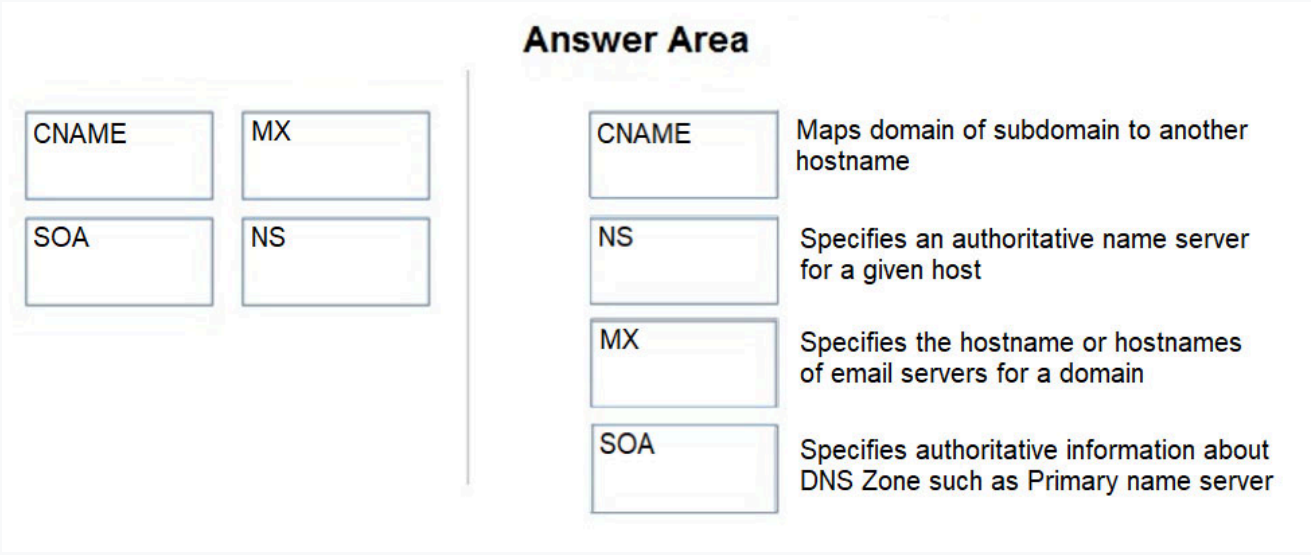
DRAG DROP -

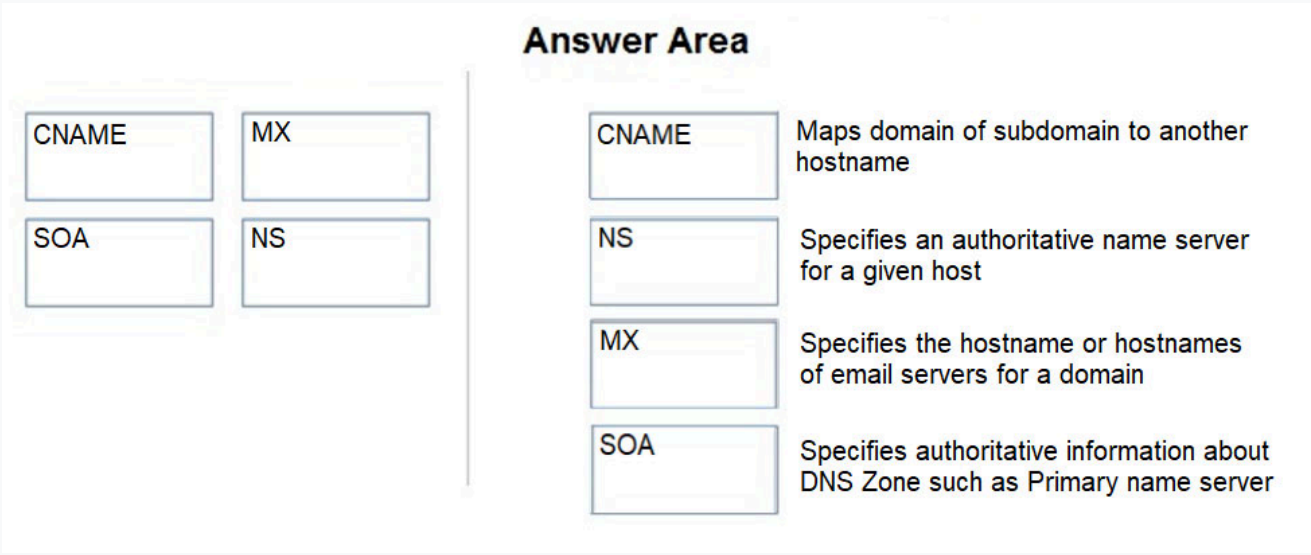
Match the DNS record type to its function within DNS.

Select and Place:



Suggested Answer:





blahblah1234567890000 1 year, 11 months ago

The basic DNS record types are as follows: ● A (IPv4) or AAAA (IPv6) (Address): Maps a domain or subdomain to an IP address or multiple IP addresses ● CNAME (Canonical Name): Maps a domain or subdomain to another hostname ● MX (Mail Exchanger): Specifies the hostname or hostnames of email servers for a domain ● PTR (Pointer): Points to a CNAME; commonly used for reverse DNS lookups that map an IP address to a host in a domain or subdomain ● SOA (Start of Authority): Specifies authoritative information about a DNS zone such as primary name server, email address of the domain administrator, and domain serial number ● NS (Name Server): The NS record specifies aan authoritative name server for a given host. ● TXT (Text): Stores text-based informationAnswer appears correct.

upvoted 3 times

blahblah1234567890000 1 year, 11 months ago

The basic DNS record types are as follows: ● A (IPv4) or AAAA (IPv6) (Address): Maps a domain or subdomain to an IP address or multiple IP addresses ● CNAME (Canonical Name): Maps a domain or subdomain to another hostname ● MX (Mail Exchanger): Specifies the hostname or hostnames of email servers for a domain ● PTR (Pointer): Points to a CNAME; commonly used for reverse DNS lookups that map an IP address to a host in a domain or subdomain ● SOA (Start of Authority): Specifies authoritative information about a DNS zone such as primary name server, email address of the domain administrator, and domain serial number ● NS (Name Server): The NS record specifies aan authoritative name server for a given host. ● TXT (Text): Stores text-based information

upvoted 3 times

blahblah1234567890000 Most Recent 1 year, 11 months ago

Answer appears correct.

upvoted 3 times

Question #84 *Topic 1*

In which phase of the cyberattack lifecycle do attackers establish encrypted communication channels back to servers across the internet so that they can modify their attack objectives and methods?

A. exploitation

B. actions on the objective

C. command and control

D. installation

Suggested Answer: *C*

Official Answer: C

Community vote distribution

C (100%)

blahblah1234567890000 Most Recent 1 year, 11 months ago

Command and Control: Attackers establish encrypted communication channels back to command-and-control (C2) servers across the internet so that they can modify their attack objectives and methods as additional targets of opportunity are identified within the victim network, or to evade any new security countermeasures that the organization may attempt to deploy if attack artifacts are discovered.

upvoted 3 times

Question #85 *Topic 1*

Which type of IDS/IPS uses a baseline of normal network activity to identify unusual patterns or levels of network activity that may be indicative of an intrusion attempt?

A. Knowledge-based

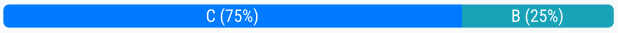
B. Signature-based

C. Behavior-based

D. Database-based

Suggested Answer: *C*
Official Answer: C

Community vote distribution



emlee Most Recent 1 year, 11 months ago
most recent PCCET study guide has the response quoted by leipeG 4 months ago; correct answer is B
upvoted 2 times

leipeG 2 years, 3 months ago
The type of IDS/IPS that uses a baseline of normal network activity to identify unusual patterns or levels of network activity that may be indicative of an intrusion attempt is: C. Behavior-based Behavior-based intrusion detection and prevention systems (IDS/IPS) analyze the behavior and activities of network traffic or systems to detect anomalies or deviations from normal behavior. They establish a baseline of what is considered "normal" and then trigger alerts or block activity that deviates from that baseline. This approach is particularly effective at identifying new or previously unseen threats that may not have specific signatures or known patterns.
upvoted 1 times

splashy 2 years, 7 months ago
"normal network activity" & "unusual patterns" are a behavior not a signature.
upvoted 1 times

csco10320953 3 years, 1 month ago
Which type of IDS/IPS uses a baseline of normal network activity -Key word baseline of normal network actvitiy - ANS: Signature Based
upvoted 1 times

blahblah1234567890000 3 years, 5 months ago
A behavior-based system uses a baseline of normal network activity to identify unusual patterns or levels of network activity that may be indicative of an intrusion attempt.Agreed https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ipsIDSs and IPSs also can be classified as knowledge-based (or signature-based) or behavior-based (or statistical anomaly-based) systems: ● A knowledge-based system uses a database of known vulnerabilities and attack profiles to identify intrusion attempts. These types of systems have lower false-alarm rates than behavior-based systems but must be continually updated with new attack signatures to be effective. ● A behavior-based system uses a baseline of normal network activity to identify unusual patterns or levels of network activity that may be indicative of an intrusion attempt. These types of systems are more adaptive than knowledge-based systems and therefore may be more effective in detecting previously unknown vulnerabilities and attacks, but they have a much higher false-positive rate than knowledge-based systems
upvoted 4 times

blahblah1234567890000 3 years, 5 months ago
Selected Answer: C
A behavior-based system uses a baseline of normal network activity to identify unusual patterns or levels of network activity that may be indicative of an intrusion attempt.
upvoted 4 times

duckduckgooo 3 years, 4 months ago
Agreed https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips
upvoted 1 times

blahblah1234567890000 3 years, 5 months ago
IDSs and IPSs also can be classified as knowledge-based (or signature-based) or behavior-based (or statistical anomaly-based) systems: ● A knowledge-based system uses a database of known vulnerabilities and attack profiles to identify intrusion attempts. These types of systems have

lower false-alarm rates than behavior-based systems but must be continually updated with new attack signatures to be effective. ● A behavior-based system uses a baseline of normal network activity to identify unusual patterns or levels of network activity that may be indicative of an intrusion attempt. These types of systems are more adaptive than knowledge-based systems and therefore may be more effective in detecting previously unknown vulnerabilities and attacks, but they have a much higher false-positive rate than knowledge-based systems

upvoted 3 times

Question #86 *Topic 1*

What differentiates Docker from a bare metal hypervisor?

A. Docker lets the user boot up one or more instances of an operating system on the same host whereas hypervisors do not

B. Docker uses more resources than a bare metal hypervisor

C. Docker is more efficient at allocating resources for legacy systems

D. Docker uses OS-level virtualization, whereas a bare metal hypervisor runs independently from the OS

Suggested Answer: *D*
Official Answer: D

Alinutzu Most Recent 1 year, 9 months ago

D. Hypervisors are of two types – the bare metal works directly on the hardware - while type two hypervisor works on top of the operating system. Docker works on the host kernel itself. Hence, it does not allow the user to create multiple instances of operating systems.

upvoted 1 times

Question #87 *Topic 1*

On which security principle does virtualization have positive effects?

A. integrity

B. confidentiality

C. availability

D. non-repudiation

Suggested Answer: *C*
Official Answer: C

Alinutzu Most Recent 1 year, 9 months ago

C. virtualization positive effects - Improved server reliability and availability

upvoted 1 times

Question #88 *Topic 1*

Which type of malware takes advantage of a vulnerability on an endpoint or server?

A. technique

B. patch

C. vulnerability

D. exploit

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

blahblah1234567890000 Highly Voted 2 years, 11 months ago

These are not types of malware, question is incorrect or answers are incorrect.

upvoted 5 times

leipeG Most Recent 1 year, 9 months ago

The type of malware that takes advantage of a vulnerability on an endpoint or server is: D. Exploit Exploits are malicious software or code that target known vulnerabilities in software, operating systems, or applications. They take advantage of these vulnerabilities to compromise or infect the targeted endpoint or server. Exploits are often used to deliver other types of malware or gain unauthorized access to a system. Options A, B, and C are related to the context of vulnerabilities and security but do not directly describe the malware that actively leverages vulnerabilities to compromise systems.

upvoted 1 times

splashy 2 years, 1 month ago

Weird question you would expect possible examples from malware So i choose D. Page 37 1.12 Differentiate between vulnerabilities and exploits An exploit is a type of malware that takes advantage of a vulnerability in installed endpoint or server software such as a web browser, Adobe Flash, Java, or Microsoft Office. An attacker crafts an exploit that targets a software vulnerability, causing the software to perform functions or execute code on behalf of the attacker.

upvoted 1 times

Syfusion 2 years, 2 months ago

Answer is D Study Guide page 32 under Exploitation phase of the Cyberattack Lifecycle "An end user may unwittingly trigger an exploit, for example, by clicking a malicious link or opening an infected attachment in an email, or an attacker may remotely trigger an exploit against a known server vulnerability on the target network. Breaking the cyberattack lifecycle at this phase of an attack, as during the Reconnaissance phase, begins with proactive and effective end-user security awareness training that focuses on topics such as malware prevention and email security."

upvoted 2 times

rob899 2 years, 5 months ago

Answer is D

upvoted 2 times

dax 2 years, 7 months ago

no correct answer. the nearest would be D

upvoted 1 times

csco10320953 2 years, 7 months ago

Ansewer :D An exploit is a code that takes advantage of a software vulnerability or security flaw. It is written either by security researchers as a proof-of-concept threat or by malicious actors for use in their operations.

upvoted 1 times

HungHa 2 years, 9 months ago

answer is D An exploit is a type of malware that takes advantage of a vulnerability in installed endpoint or server software such as a web browser, Adobe Flash, Java, or Microsoft Office

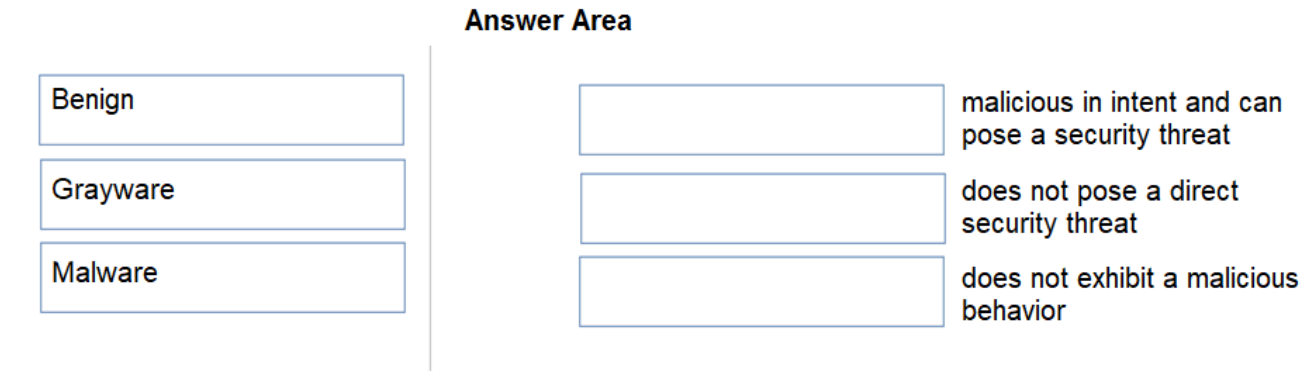
upvoted 2 times

Question #89 *Topic 1*

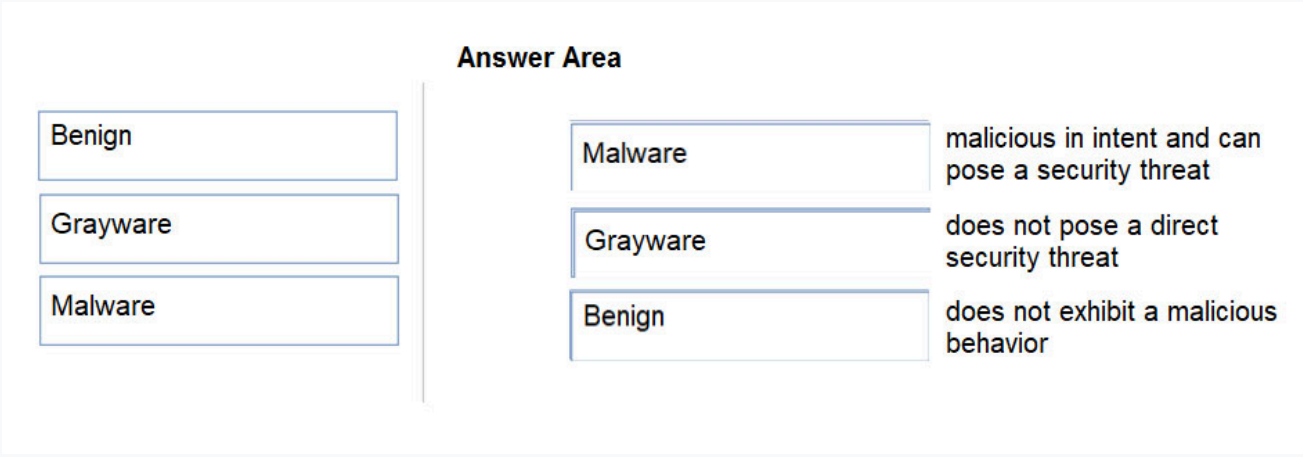
DRAG DROP -

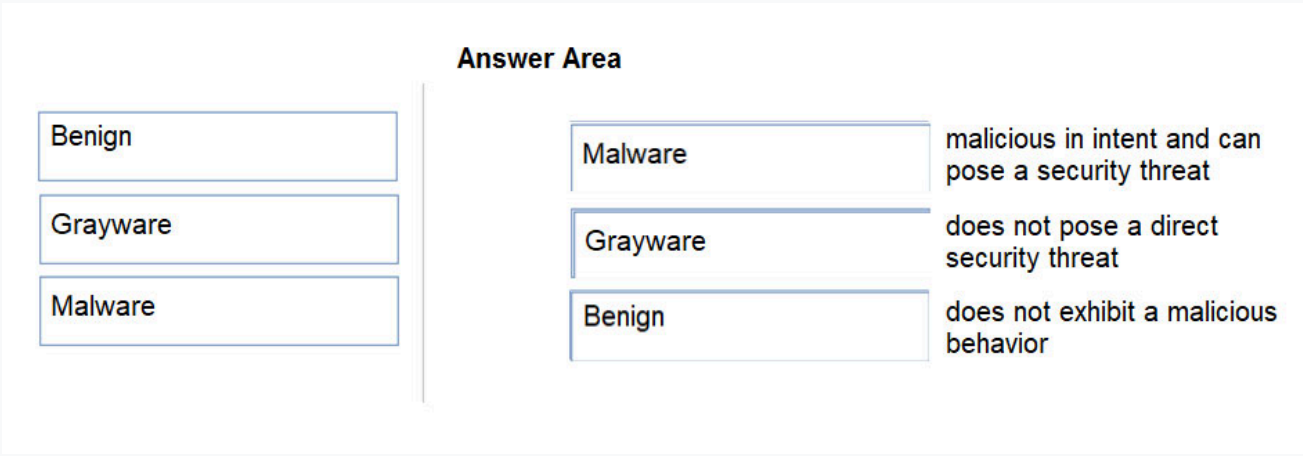
Match the Palo Alto Networks WildFire analysis verdict with its definition.

Select and Place:



Suggested Answer:





blahblah1234567890000 Most Recent 1 year, 11 months ago

Possible verdicts include: ● Benign: Safe and does not exhibit malicious behavior ● Grayware: No security risk but might display obtrusive behavior (for example, adware, spyware, and browser helper objects) ● Malware: Malicious in nature and intent and can pose a security threat (for example, viruses, worms, trojans, root kits, botnets, and remote-access toolkits) ● Phishing: Malicious attempt to trick the recipient into revealing sensitive data

upvoted 3 times

Question #90 *Topic 1*

What protocol requires all routers in the same domain to maintain a map of the network?

A. EIGRP

B. Static

C. RIP

D. OSPF

Suggested Answer: *D*
Official Answer: D

Alinutzu Most Recent 1 year, 9 months ago

D. The protocol that requires all routers in the same domain to maintain a map of the network is the "Link State Routing Protocol." In a link state routing protocol, each router in the network maintains a detailed map of the network's topology. This map includes information about all the routers in the network, the links between them, and various metrics or costs associated with those links. The most common example of a link state routing protocol is the Open Shortest Path First (OSPF) protocol.

upvoted 1 times

Question #91 *Topic 1*

A doctor receives an email about her upcoming holiday in France. When she clicks the URL website link in the email, the connection is blocked by her office firewall because it's a known malware website. Which type of attack includes a link to a malware website in an email?

A. whaling

B. phishing

C. pharming

D. spam

Suggested Answer: *B*
Official Answer: B

duckduckgooo Most Recent 1 year, 10 months ago

B is correct

upvoted 1 times

Question #92 *Topic 1*

With regard to cloud-native security in layers, what is the correct order of the four C's from the top (surface) layer to the bottom (base) layer?

A. container, code, cluster, cloud

B. code, container, cluster, cloud

C. code, container, cloud, cluster

D. container, code, cloud, cluster

Suggested Answer: *B*
Official Answer: B

Alinutzu Most Recent 1 year, 9 months ago

C. code, container, cloud, cluster This order represents the typical approach to securing cloud-native applications, starting with the security of the application code, followed by container security, cloud platform security, and finally, the security of the underlying cluster or orchestration environment.

upvoted 1 times

duckduckgooo 2 years, 10 months ago

I've seen multiple pages showing Cloud/Cluster/Container/Code - so none of the above https://kubernetes.io/docs/concepts/security/overview/ https://containerjournal.com/features/the-four-cs-of-cloud-native-security/

upvoted 1 times

Question #93 *Topic 1*

Under which category does an application that is approved by the IT department, such as Office 365, fall?

A. unsanctioned

B. prohibited

C. tolerated

D. sanctioned

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

blahblah1234567890000 Most Recent 1 year, 11 months ago

● Sanctioned (allowed and provided by IT) ● Tolerated (allowed because of a legitimate business need, with restrictions, but not provided by IT) ● Unsanctioned

upvoted 1 times